Obsidian IT
Simple / Scalable / Outsourced IT

flexIT [User] Master Service Agreement

(MSA) + Technical Alignment

Created 11/02/2026 | **Quote Number:** 21069

Prepared for:
Burney Water District
David Zevely | dzevely@burneywaterdistrict.org
20222 Hudson Street
Burney, California 96013, United States

Prepared by:
Nikki Anthony | NAnthony@ObsidianIT.com
Valid until 11/30/2026

Master Service Agreement (MSA) + Technical Alignment

flexIT offers flexible, cost-effective access to expert support and core security solutions for troubleshooting, maintenance, and protection.

Benefits:

- **Clear Expectations:** Defines services and performance standards.
- **Proactive Support:** Prevents issues, minimizing downtime.
- **Cost Efficiency:** Fixed monthly fees reduce unexpected costs.
- **Enhanced Security:** Regular updates protect against threats.
- **Access to Expertise:** Specialized IT knowledge and skills.
- **Scalability:** Adjusts to your business's needs.

Obsidian IT's flexIT Contract:

- **Adaptive Services:** Adjusts to changing needs.
- **Customer Profile:** Updates user, device, and software counts monthly.
- **Semi-Managed Service:** Flexible support and security solutions.
- **flexIT Support:** Unlimited Remote and Onsite Support, Monday to Friday, 7 am to 5 pm, with a 20% discount on professional services.

An MSA with Obsidian IT ensures proactive, efficient, and secure IT management, allowing you to focus on your core business.

Burney Water District Customer Profile

Businesses are dynamic, and your IT contract should be too! With our **flexIT** contract, your IT services adapt seamlessly to your business's changing needs. Whether you're experiencing a seasonal shift with fewer staff or enjoying growth and success, your contract adjusts to meet your current requirements. Your Customer Profile outlines the number of users, devices, and software essential for your operations. Our system automatically adjusts these counts every month, ensuring you always have the right resources. Below are the current counts found during discovery.

Assumptions	Quantity
Number of flexIT Support Hours	Unlimited
Number of named users	5
Microsoft M365 or Google Workspace Email Accounts (e.g., you@yourcompany.com)	8
Non-business email accounts	
Workstations or Laptops	6
Server (Stand Alone)	1
VM Host (Physical Machine)	
VM Guest	
Routers / Firewalls	1
Wi-Fi Wireless Access Points (WAPs)	1
Switches	1
VPNs	
PDUs	
NASs	TBD
UPSs	TBD
Domains	1

"Cybersecurity isn't about one tool—it's about layered protection, continuous monitoring, and fast response."

Obsidian IT's First in Class Security

Remove the Complexity of Multi-Layered Security Offering

With the ever-increasing number of devices connected to IT networks, the pathway for malicious actors is expanding by the second. A trustworthy defense requires sophisticated security tools that can detect and address even the most advanced cyberthreats before they become a problem. Obsidian IT Security Solutions provide full coverage while also being simple to manage, providing Business Professionals both peace and ease of mind.

$16.6 billion That is the total reported financial loss in the United States in 2024, according to the FBI's Internet Crime Complaint Center (IC3).	**$78,000 - $254,000** is the average spend of SMBs to restore business in the wake of a cyber attack.	**1 in 3 SMB's** experienced a cyberattack in the last year. This comes directly from recent Microsoft SMB research.
32% of ransomware attacks result from unpatched software.	**248+** new vulnerabilities are disclosed each day, based on CVE data from 2026.	**Every Second** 19 ransomware attempts occur worldwide.





Endpoint Security Stack

- Monitoring, Patch Management
- Ransomware Detection
- Anti-Virus Software
- DNS Filtering
- EDR (Endpoint Detection Response)

Email Filtering for M365 and Google Workspace

Uses advanced AI-powered threat detection to protect your organization from phishing, ransomware, impersonation, and other email-based attacks. By analyzing every email, identifying suspicious content, and providing users with clear visual warnings, INKY helps prevent cybercriminals from gaining access to your systems, data, and accounts while strengthening your overall security posture.

Inky for M365 and Google Workspace



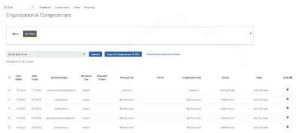


Security Awareness Training

BullPhish ID helps educate employees to recognize phishing, social engineering, and other threats, transforming your workforce into an active and informed security defense layer.

Dark Web Monitoring

Dark Web ID watches the parts of the internet criminals use—so if your company's credentials are stolen, we know immediately and can secure accounts before attackers get in.



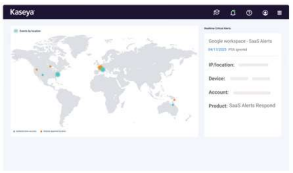


24/7 Managed SOC Team

Obsidian IT's 24/7 Managed SOC protects your business by continuously monitoring your systems for real threats, filtering out noise, and bringing security experts into the fight before small issues turn into major incidents.

24/7 SaaS Alerts

SaaS Alerts protects your most critical business systems—like Microsoft 365, Google Workspace and cloud apps—by detecting suspicious user behavior in real time and automatically stopping account-based attacks before they turn into downtime, data loss, or ransomware.



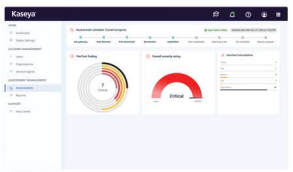


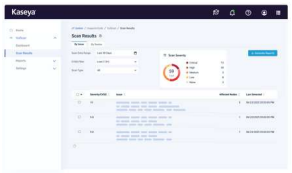
24/7 SaaS Back Up for M365 and Google Workspace

Automatically backs up your cloud-based emails, documents, calendars, contacts, and collaboration data multiple times per day. By maintaining secure backup copies independent of Microsoft and Google, your organization can quickly recover from accidental deletions, ransomware, cyber incidents, and retention policy issues while supporting business continuity, regulatory compliance, and peace of mind.

Automated Network Penetration Testing

Simulates real-world cyberattacks against your network to identify exploitable vulnerabilities before criminals do. By proactively uncovering weaknesses, prioritizing risk, and providing actionable remediation guidance, penetration testing helps strengthen your security, reduce exposure to cyber threats, and support compliance requirements.





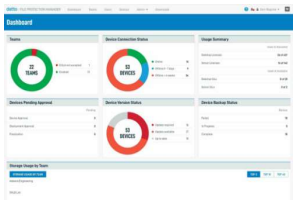
Vulnerability Scanning

Continuously identifies security weaknesses across your network, servers, workstations, and connected devices. By uncovering vulnerabilities, missing patches, and configuration issues before they can be exploited, your organization can prioritize remediation efforts, reduce cyber risk, improve compliance readiness, and maintain a stronger security posture across every endpoint.

24/7 SIEM

SIEM helps SMBs cut response time by automating routine containment actions—shrinking tasks that often take minutes manually into near-immediate, policy-driven responses—before incidents turn into downtime.





7 Day Rollback Protect Against Ransomware

In today's rapidly evolving threat landscape, fast recovery is critical for workstation environments after ransomware attacks or system failures. Minimize downtime and data loss by ensuring your data remains protected and untouchable—whether threats come from cybercriminals or accidental user actions.

You Can’t Manage Risks You Don’t Know About

Without the right information, managing risks and ensuring compliance with your IT requirements is impossible. Our team simplifies this process by maintaining complete visibility of your growing network, prioritizing security measures, and documenting compliance. With our **Alignment, Standardization and Collaboration (ASC)** Service, you are assigned a dedicated Technical Alignment Manager (**TAM**) and Virtual Chief Information Officer (**vCIO**). Together, they will assess the health of your network infrastructure, identify risks, and align it with your industry-specific requirements. They will also assist with long-term strategy planning, budgeting, and building a strategic relationship for your business’s technology success.



Virtual Chief Information Officer (**vCIO**) Todd Davis



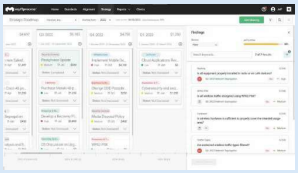
Technical Alignment Manager (**TAM**) Matthew Scott



Technical Alignment Manager (**TAM**) Austin Ely

myITprocess

With myITprocess you can effortlessly turn IT risks into a business planning roadmap.





Network Detective Pro

Network Detective Pro automatically collects data from every device on your network, then identifies and remediates issues based on objective risk scores.

Discover Hidden Vulnerabilities

With over 50 new vulnerabilities daily, VulScan simplifies hardening your IT environment. Perform internal and external scans easily, choosing when, how often, and which devices to scan.





IT Audit & Compliance Management for All

IT professionals aren't compliance experts, but they're expected to ensure safety and compliance. Kaseya Compliance Management automates dozens of standards, letting IT pros focus on their core expertise.

"Without execution, strategy is just theory." — Morris Chang

One-Time Project: Onboarding and Site Cleanup — $450.00

Product	Quantity	Price	Amount
Professional Services Estimated Time for Onboarding and Site-Cleanup: 5 hours Number of Workstations: 6 - Travel Time: 2.25 Hours -3.75 Hours: Preboarding and Onsite Onboarding Step 1: Provisioning Process Step 2: Collect all Infrastructure Information Step 3: Training Process Step 4: Service Go-Live Step 5: Report Improvements Step 6: Site Clean-Up (TBD) Please Note: This Rate is discounted from our standard rate of $145.25 (48.4% Discount)	6	$75.00	$450.00

flex IT User Plan for Named Users — $800.00

Product		Quantity	Price	Amount
Managed User(s) (MSA)+(ASC) for Help, Remote, Onsite, Centralized Service, Alignment, Standardization, and Collaboration Services. Excludes: Project, Moves, Major Software Updates, and Disaster Recovery. Includes: -Endpoint Security Stack -Email Security -(SOC) Security Operations Center -Awareness Email Phishing -Dark Web Email Monitoring -SaaS Cloud Detection for M365 & Google Workspace -(SIEM) Security Information and Event Management -SaaS Back Up for M365 & Google Workspace -Automated Network Penetration Testing (vPen) per IP Address -Vulnerability Scanning Managed Users Defined As: 1) David Z. 2) Stephanie M. 3) Maggie A. 4) Cedalia T. 5) Field Staff Workers (Minimal Workstation Use)	Monthly x 12	5	$160.00	$800.00

flex IT Security Tools Essential		$0.00
Product		**Quantity**
S1Security: Endpoint Security Stack -Monitoring, Patch Management -Ransomware Detection -Anti-Virus -DNS Filtering -EDR (Endpoint Detection Response) -Ransomware Rollback -Standard Price $10.80 per user	Monthly x 12	8
S2Security: Email Security -For M365 and Google Workspace Email Filtering -Standard Price $3.33 per user **For All Licensed User Emails**	Monthly x 12	8
S3Security: SOC (Security Operation Center) Stack -SOC (Security Operation Center) 24/7 -SOC (Security Operation Center) Email -Standard Price $2.50 per user	Monthly x 12	8
S4Security: Security Awareness Email Phishing -Standard Price $3.00 per user **For All Licensed User Emails**	Monthly x 12	8
S5Security: Dark Web Personal Email Monitoring -Standard Price $.50 per user **For All Licensed User Emails and Dark Web**	Monthly x 12	9
S10Security - SaaS Alerts Cloud Detection Platform for M365 & Google Workspace -Standard Price $3.60 per user **For All Licensed User Emails**	Monthly x 12	8
S16Security - Security Information and Event Management (SIEM) -Standard Price $3.33 per user **For All Licensed User Emails**	Monthly	8
S8Unified Backup - SaaS Backup Protection -Standard Price per M365 or Google Workspace $3.60 per email **For All Licensed User Emails**	Monthly	8
S12Audit and Compliance - Network Penetration Test (vPen) per IP Address -Standard Price $5.61 per external IP address	Monthly	1
S15Audit and Compliance - Vulnerability Scan -Standard Price $40.00 per organization	Monthly	1

Monthly Backup Reccurring Licensing **$60.00**

Product		Quantity	Price	Amount
S7Unified Backup - Endpoint Backup Protection Per 500GB Storage TBD: Will determine from on-site visit -Hosts Billmaster -Hosts QuickBooks -Not Leveraging OneDrive yet	Monthly x 12	4	$15.00	$60.00

Other Monthly Reoccurring Licensing **$8.40**

Product		Quantity	Price	Amount
OIT-Microsoft Entra ID P1 -(1) License per organization -For M365 Users Only (Not needed if using Premium Licenses) -This license provides advanced security and identity management features that allow us to implement stronger security policies, improve access controls, and better protect your organization from modern cyber threats. It also enables us to more effectively harden your Microsoft 365 environment and align it with current security best practices.	Monthly	1	$8.40	$8.40

One Off	$450.00
Monthly	$868.40
Shipping	$0.00
Tax	$0.00
Total	**$1,318.40**

Included Agreements & Conditions:

- **Master Service Agreement (MSA): Version 9.1.25**
- **Service Level Agreement (SLA)**
- **Standard Rate**
- **Terms and Conditions**
- **Hardware as a Service (HaaS) Addendum: Version 3.4.26**
- **Backup, Data Residency, and Client Responsibility Agreement: Version 6.1.26**

Getting Started and Support Resources:

- **Creating Tickets and My Support Team**