tdi vertical

TECHNOLOGY DRIVEN INNOVATION

City of Waukesha

Cybersecurity Support Services

SOW # 55104

01/08/2026

Contents

1. EXECUTIVE OVERVIEW

1.1. Terms and Conditions

Once executed by both parties, this Statement of Work becomes effective and is covered by General Terms outlined in the Master Services Agreement executed between the parties.

In the event of a conflict between the Master Services Agreement and this Statement of Work, the order of precedence will be this Statement of Work and then the Master Services Agreement.

Either party may terminate this Statement of Work, without cause, by providing thirty (30) days' prior written notice to the other party. Upon termination, Client shall pay TDI Vertical for all services performed and expenses incurred up to the effective termination date. Any prepaid amounts for services not yet rendered shall be refunded to Client within thirty (30) days of termination. Termination of this Statement of Work does not affect any obligations under the Master Services Agreement unless otherwise agreed in writing by both parties.

1.2. Contact Information

CITY OF WAUKESHA		TDI VERTICAL LLC
Chris Pofahl Director of IT 262.524.3566 cpofahl@waukesha-wi.gov		Peter Jedrocha Customer Success Manager 847.652.4876 pjedrocha@tdivertical.com Stan Hyrczyk CTO, Lead Architect 224.716.3510 shyrczyk@tdivertical.com

1.3. Cybersecurity Support Overview

TDI Vertical offers comprehensive Cybersecurity support services for businesses of all sizes. With a team of experts, our services ensure the smooth operation of all IT systems, networks, and security services.

The objective of this SOW is to provide specialized, expert-level support as needed to enhance Client's IT operations without the commitment of a full-time IT team.

By partnering with TDI Vertical, organizations gain access to industry-leading expertise, ensuring that both cybersecurity and IT infrastructure needs are met with precision and care, ultimately empowering business growth and operational success.

Requested services will be performed based on a Time and Materials pricing model.

All services will be billed as incurred and invoiced monthly.

1.4. Why Choose TDI Vertical?

Security Focused

At TDI Vertical, we understand the importance of cyber security. Our security-first approach is critical to the success of our customers and the longevity of their business. By prioritizing security, we minimize the risk of exposure and protect our customers against modern-day cyber security threats, including data breaches, malware attacks, phishing scams, and ransomware attacks.

Proven Experience

With extensive experience in information technology, TDI Vertical understands business challenges with technology, the latest trends, tools, and solutions. As a trusted advisor, our team provides our customers with

valuable insights and recommendations based on our knowledge and industry experience, focusing on business needs, strategy, and growth.

Innovation Driven

As an innovation-driven solution provider, TDI Vertical follows a strategic approach to technology selection that involves identifying and evaluating emerging technologies that can provide unique solutions to business challenges. This approach goes beyond traditional technology evaluation methods and focuses on identifying innovative and disruptive technologies that can drive business growth and transformation.

1.5. Service Locations

Work will be done at the following locations. All work will be performed remotely unless otherwise specified.

Site Name	Address	On-Site / Remote
City of Waukesha	201 Delafield St. Waukesha, WI 53188	Remote

2. CYBERSECURITY SUPPORT

2.1. Project Scope

TDI Vertical will deliver Cybersecurity Support Services as an extension of the Client's cybersecurity team. This engagement includes continuous monitoring, management, investigation, and escalation of alerts within the Client's Microsoft Sentinel SIEM environment. TDI Vertical will perform threat hunting, incident investigation, cross-platform log analysis, and assist with remediation efforts as needed to ensure rapid response and operational stability. In the event of the termination of this Statement of Work, any Playbooks developed, created, or added to the City's SIEM environment is considered property of the City and will remain in the City's SIEM environment.

Upon request, TDI Vertical will also provide engineering expertise for ad hoc cybersecurity tasks outside of Sentinel SIEM monitoring.

This service will be delivered on a time-and-materials basis with full 24-hour coverage**.**

- **Microsoft Sentinel SIEM Monitoring & Management**
  - 24/7 monitoring of Microsoft Sentinel SIEM alerts and events.
  - Management of SIEM-related tickets and incidents.
  - Continuous triage, investigation, and analysis of SIEM alerts.
  - Classification, prioritization, and documentation of all alerts and incidents.
  - Development, tuning, and optimization of Sentinel detection rules as needed.
- **Threat Hunting & Incident Investigation**
  - Proactive threat hunting within Microsoft Sentinel SIEM.
  - In-depth investigation of security alerts, anomalies, and suspicious activity.
  - Root cause analysis (RCA) for identified incidents.
  - Correlation of signals across multiple security and system sources.
- **Cross-Platform Log Review & Analysis**

  As part of investigations, TDI Vertical will review additional logs when necessary, including:
  - Firewall/network appliance logs
  - Endpoint protection and EDR logs
  - Server and system logs
  - Cloud security logs (if applicable)

- Identity, authentication, and access logs

- **Escalations & Communications**
  - Immediate escalation to Client for critical or high-severity events.
  - Structured handoff of incident details, recommended actions, and impact assessment.
  - Notifications via Client-approved communication channels.
  - All SIEM alerts and security events will be forwarded to TDI Vertical's ticketing system for tracking.
- **Meetings & Reporting**
  - Weekly operational meetings to review recent alerts, incidents, and ongoing investigations.
  - Monthly service review meetings to discuss KPIs, recurring issues, and service improvements.
  - Summary reporting for tickets, incidents, trends, and recommendations.
- **Playbook Development**
  - Creation and improvement of Microsoft Sentinel incident response playbooks.
  - Documentation of workflows, escalation paths, and remediation steps.
  - Continuous refinement based on incident learnings and Client feedback.
- **Remediation Assistance**
  - Hands-on support to assist with remediation of cybersecurity incidents.
  - Support to restore affected firewall, network, endpoint, system, and server services to fully operational state.
  - Collaboration with Client's internal teams for containment, eradication, and recovery effort
- **Ad-Hoc Engineering Support**
  - Provide engineering resources for tasks outside of daily SIEM monitoring.
  - Act as the subject matter expert (SME) and consult the Client on network, wireless, security, and systems architecture best practices, design, and modernization strategy.
  - Provide ad/hoc technical support for Network, Security, Systems including but not limited to Virtualization, Data Protection, Storage, Microsoft Active Directory, Windows Servers, and Microsoft O365-related matters.
  - Assist with configuration, troubleshooting, change control, and improvements of network, security, and systems infrastructure.
  - As needed, host technical workshop/s with the Client to discuss current architecture, recommendations for improvements, growth strategy, etc.
  - When required, assist in developing change control and implementation playbook/s and work with the Client on execution.
  - When applicable, maintain network and systems documentation, including diagrams related to the overall architecture.

2.2. Technical Resources

Technical resources are assigned based on technical requirements of the scope, skillset, and an overall experience of resources with the technology and the solution being implemented.

To fulfill the technical requirements of this scope, TDI Vertical will assign the following resources.

Resources	Description	Duration (Full-time/Part-time)
Security Analyst/s	Security Analyst/s responsible for monitoring and managing Microsoft Sentinel SIEM, including alert	Full-time

	triage, incident analysis, rule tuning, log ingestion oversight, dashboard/report updates, threat hunting, and maintaining SIEM configurations to enhance overall security posture.	
Sr. Security Engineer	Sr. Security Engineer responsible for security aspects of the project including but not limited to firewall troubleshooting, tuning, optimization, miscellaneous configuration, etc.	Part-time
Sr. Wireless Engineer	Sr. Wireless Engineer responsible for wireless aspects of the project including but not limited to troubleshooting of wireless controllers, tuning, optimization of WLANs, configurations, etc.	Part-time
Sr. Network Engineer	Sr. Network Engineer responsible for technical aspects of the project including but not limited to troubleshooting of network, tuning, optimization of, configurations, etc.	Part-time
Sr. Systems Engineer	Sr. Systems Engineer responsible for technical aspects of the project including but not limited to troubleshooting of systems, storage, tuning, optimization of, configurations, etc.	Part-time

2.3. Project Change Order Process

A Project Change Order is required for all out-of-scope or additional services not listed under the *"Project Scope"* section of this Statement of Work.

When required, Project Change Order will be developed by TDI Vertical, documenting all additional services being requested.

Project Change Order must be reviewed and approved by the Client prior to any work or services being performed by TDI Vertical.

3. PROJECT ASSUMPTIONS

Project assumptions in this Statement of Work serve as the foundation to which the project estimate, approach, and timeline were developed by TDI Vertical.

With the approval of this Statement of Work, Client agrees to these assumptions and confirms that these are valid.

Any changes to the outlined assumptions require a Project Change Order and may increase the cost of services provided.

3.1. Project Specific Assumptions

1. Client understands the estimated hours are only an estimate and that additional hours may be required to complete all activities listed under *"Project Scope"*
2. All additional time and overages are billed based on the Time and Materials pricing model and invoiced monthly.
3. 24/7 Monitoring and Management of Microsoft Sentinel SIEM
4. Client owned Microsoft Sentinel SIEM
5. Client to provide access to Microsoft Sentinel SIEM
6. When needed Client to provide access to Firewalls.
7. When needed, Client is to provide access to network-related devices.
8. Client to provide an escalation matrix for any high and critical alerts and incidents.

9. Client to participate in any P1/Critical incidents.
10. All incidents and alerts are forwarded to the TDI Vertical ticketing system.
11. All time billed in 30-minutes Increments.
12. TDI Vertical assumes a minimum of four (4) hours for each on-site service call.
13. Travel time will be added for each on-site service call.
14. All support requests should be directed to support@tdivertical.com
15. Excludes Cybersecurity Incident Response Services.
16. Premium SLAs and a 30-minute response time apply to all critical incidents and alerts.
17. Standard SLAs apply to all other non-critical incidents and alerts.

3.2. General Assumptions

General Project Assumptions outline general assumptions made by TDI Vertical when developing this Statement of Work.

1. Any items, tasks, or activities not explicitly listed under the "*Project Scope"* section of this Statement of Work are outside of the scope and will require Project Change Order to account for additional time and engineering efforts.
2. Any changes to the solution design, or proposed timeline presented to and approved by Client during planning and design phase, will require a Project Change Order to account for additional time and engineering effort.
3. TDI Vertical will not be held responsible for troubleshooting networks, applications and/or hardware if Client has no formal change management documented processes and policies.
4. At any time, TDI Vertical may engage a third party or subcontractors to perform a portion of the agreed-upon services.
5. TDI Vertical will not make changes to the configuration of any network equipment after it has been installed and tested.
6. During execution of services, all hardware, software, or cloud base solution or services will be configured with a unique set of TDI Vertical authentication credentials unless otherwise provided by Client.
7. Upon completion of all services, TDI Vertical will provide Client with all access credentials previously configured and used by TDI Vertical technical resources.
8. TDI Vertical assumes that services provided under this Statement of Work will be performed during normal working hours (8:00 a.m. to 6:00 p.m. Central Standard Time). Due to the nature of work being performed, on some occasions and with reasonable advance notice, Client may need to provide access to its facilities outside of these hours.

3.3. General Client Responsibilities

General Client Responsibilities outlines all items and activities that Client is responsible for.

1. Provide a single point of contact with the authority and the responsibility of issue resolution and the identification, coordination, and scheduling of Client personnel to participate in the implementation of the SOW.
2. Participate in all projects related calls and workshops including but not limited to project kickoff, status calls, design sessions, implementation planning, solution deployment, test and acceptance, validation, and day one post support.
3. Provide any required hardware, licensing, support, and subscription services required to support execution of services outlined under *"Project Scope"* section of this Statement of Work.
4. Handle internal change control process and change communication throughout the duration of this project.
5. Coordinate and schedule appropriate change control windows for any services performed by TDI Vertical.
6. Maintain valid manufacturer support contracts for hardware, and network devices related to services outlined under *"Project Scope"* section of this Statement of Work.

7. When required, provide TDI Vertical with physical access to Client's facility.
8. When required, provide TDI Vertical with an identification badge, onsite escort, parking permit, etc.
9. When applicable, perform validation of site readiness prior requesting TDI Vertical for onsite services.
10. Review and approve results from test and acceptance procedures.
11. When requested, provide TDI Vertical with technical documentation related to the current state of the infrastructure.
12. Provide remote access VPN, and network access credentials to all TDI Vertical technical resources assigned to this project.
13. When required provide TDI Vertical access to internal monitoring systems, Active Directory Domain Controllers, DHCP servers, DNS servers, etc.
14. When required, provide adequate facilities, rack space, power, and cooling to support installation of hardware.
15. When required, provide TDI Vertical with all necessary peripherals to complete execution of services. This includes but is not limited to KVM, monitors, keyboards, mice, network access, etc.
16. When required, transport network equipment to all service locations listed under *"Executive Overview"* section of this statement of Work.
17. Provide adequate low-voltage, fiber, and structure cabling required to support execution of services outlined under *"Project Scope"* section of this Statement of Work.
18. Provide required copper and fiber optic patch cords as well as transceivers.

4. PRICING

Any changes to this Statement of Work require Project Change Order and may incur additional charges.

Services provided under this Statement of Work are based on the Retainer pricing model and invoiced in full upon execution of this contract.

TDI Vertical payment terms for services performed under this Statement of Work are Net-30.

Cybersecurity Support Services - Retainer	Hours	Rate	Cost
Cybersecurity Support Services*	50	$205.00	$10,250.00
Total Estimated Cost for Cybersecurity Support Services*	**50**	**$205.00**	**$10,250.00**

Invoicing Milestones - Retainer	Amount
Execution of Contract (100%)	$10,250.00
Total Estimated Cost for Cybersecurity Support Services *	**$10,250.00**

*Pricing does not include any applicable Federal, State, and local Taxes, surcharges, and Fees.

5. APPROVAL

By signing this Statement of Work, each of the signatories acknowledges their authority to bind their respective organizations to this SOW and the Master Services Agreement.

This Statement of Work is valid for a period of thirty (30) days from the date that this Statement of Work is provided unless otherwise agreed to by both parties.

City of Waukesha

Signature Date

CHRIS POFAHL, Director of IT

Printed Name & Title

TDI Vertical, LLC

Signature Date

STAN HYRCZYK, CTO

Printed Name & Title