Retained Earnings Options

	Using 100% of available Retained Earnings	Using 50% of available Retained Earnings	Notes
Available Funds	$558,257.10	$279,128.55	
Budget Stabilization	$75,000.00	$75,000.00	Fund balance
	$249,379.00	$124,689.50	Retained Earnings (cash)
CIP Contribution	$154,439.05	$77,219.50	50% of balance after budget stabilizatior
Balance to Surplus	**$154,439.05**	**$77,219.55**	

Borrowing options based on above retained earnings usage

CIP Borrowing	$701,964.55	$779,184.10
EOY Borrowing	$0.00	$124,689.55

	COER Levy Total		Assessed Value	Mill Rate Proposed 2025	Mill Rate 2024	Difference	Mill Rate Estimated Overall
Borrowing EOY at 100% $249,379	$ 2,179,258.39	/	$ 307,333.80	7.090851681	6.188516707	0.90	10.97368699
Borrowing EOY at 50% $124,690	$ 2,031,621.17		$ 307,333.80	6.610471003	6.188516707	0.42	10.49330631
EOY Borrow 0% - Retained Earnings	$ 1,883,982.77		$ 307,333.80	6.130086473	6.188516707	-0.06	10.01292178

2024 Overall 10.1922286

Robin Ginner

From: Cory Hoffmann
Sent: Friday, October 31, 2025 11:42 AM
To: Robin Ginner; Becky Bolte; COER Mayor
Subject: EOY Loan

Importance: High

Here are the rates I have received for the EOY borrowing:

Nicolet Bank	4.89	No Fees
Incredible Bank	5.15	No Fees
Peoples Bank	5.92	Attorney Review Fee of $450.00

Thank you.

Corinne (Cory) Hoffmann
Corinne Hoffmann
Treasurer/Deputy Clerk
City of Eagle River
525 East Maple Street
P.O. Box 1269
Eagle River, WI 54521

715-479-8682 ext. 222
715-525-2664 (mobile)

2026 CIP Borrowing

701,964.55 or $779,184.10

↓ Financial Institution / Terms →	10 Years	15 Years	20 Years	PrePayment	Fees	Notes
BCPL	5.50%	6.25%	6.25%			
Incredible	5.50%	6.00%	6.50%	No penalty	$0	Semi Annual Payments (6 or 12 months after closing
Nicolet	5.49%	Balloon rates, or refinance		No penalty	$250	Semi Annual Payments (6 months after closing)
Peoples						

IT/Phone/Internet Services Quotes - 2025

	Internet							Phones							IT Services					
	City Hall	Police Dept	PD - Cameras	L&W	DPW	Golf	SYNOPSIS	City Hall	Police Dept	L&W	DPW	Golf	Airport	SYNOPSIS	City Hall	Police Dept	DPW	Golf	Grant Assistance	SYNOPSIS
*** RECOMMENDED* Frontier** *- did onsite engineering*	$69.99/mo + $10/mo wifi (1GB service)	$94.99/mo + $10/mo wifi (2GB service)	$84.99/camera location (total: $424.95/mo.) (1GB service)	$209.97/mo + $40/mo wifi (1GB service)	$69.99/mo + $20/mo wifi (1GB service)	$139.98/mo + $25/mo wifi (1GB service)	**Internet Service is $1,114.87/mo for all departments.** Least expensive internet svc. Rates for three years, then up for renewal. If we need static IP addresses, those will be $20/month extra per IP. 1 and 2GB service	$109.49/mo + $137.50 set up	$384.40/mo + $275 set up	$148.75/mo + $192.50 set up	$70.25/mo + $110 set up	$134.75/mo + $192.50 set up	$50.25/mo + $82.50 set-up	**Phone service would be $897.89/month for all departments, with an initial set up at $990.** This includes leasing phones, but we can purchase them if we wish.	n/a	n/a	n/a	n/a	n/a	---
Norvado - *did onsite inventory*	$109.99/mo.	$789.93/mo (Incl. cameras)		$329.97/mo.	$109.99/mo.	$219.98/mo.	Internet Service is $1,559.86/mo for the entire City. 1 GB service	$359.93/mo. + $0 set up (Incl. $27.95 discount if internet customer)	$823.65/mo. + $0 set up (Incl. $27.95/line discount if internet customer) **Incl 5 cameras**	$659.89/mo. + $0 set up (Incl. $27.95 discount if internet customer)	$259.95/mo. + $0 set up (Incl. $27.95 discount if internet customer)	$600.89/mo. + $0 set up (Incl. $27.95 discount if internet customer)	$403.88/mo. + $0 set up (Incl. $27.95 discount if internet customer)	Highest cost/mo ($3,108.19/mo for all departments). Will update all wiring at no cost to the CIty to make use of the ligher 1 GB speeds for internet.	n/a	n/a	n/a	n/a	n/a	---
Spectrum - *did onsite inventory*	$254/mo.	$254/mo.	can't support cameras	$254/mo.	$254/mo.	$508/mo.	Internet Service is $1,524/mo for the entire City. Cannot support cameras for PD.	$432/mo.		$81/month	$123/mo.	$195/mo.	$99/mo.	Phone service would be $930/mo for all departments. The only phone cost is for cordless phones. They can also handle our landlines if needed.	n/a	n/a	n/a	n/a	n/a	---
*** RECOMMENDED* IT Strategies**	n/a	n/a	n/a	n/a	n/a	n/a	---	$1,000 total ($25/phone connection x 40 phones city wide) - We could purchase our own phones (under the Wisconsin State Purchasing Program), though we can continue using our existing devices for the time being. Alternatively, phones can be leased through IT-Strategies if preferred. Existing phone numbers can be ported over. If we want to get new phones (or lease them) that would be an additional charge						Only support phones if we go with their IT pkg	$2,236/mo. (and goes up approximately $200/year) + $4800 (max) set up.				Yes	$26,832/year + $4800 set up (max)
VC3	n/a	n/a	n/a	n/a	n/a	n/a	---	n/a	n/a	n/a	n/a	n/a	n/a	---	$3925.90/mo. + $3,760 set-up.				Yes	$47,110.80/year + $3,760
WIN	n/a	n/a	n/a	n/a	n/a	n/a	---	n/a	n/a	n/a	n/a	n/a	n/a	---	$2155.50/mo for all City & PD IT + $11,375 set up	$10,360 set up	included in city hall	included in city hall	No	$25,866/year + set up with substantially higher than other quotes - $21,735 up front exp

Locations:	
City Hall	525 W. Maple Street – City Hall, Police Dept 15,919 sq ft
Light & Water (no IT Svcs)	511 W. Mill Street – Light & Water Shop 16,560 sq ft
	323 W. Division Street – Light & Water Wastewater Treatment Plant 5,348 sq ft
	525 W. Maple Street – Light & Water XXX sq ft
DPW	1020 N. Bluebird Road – Dept Public Works Shop 10,125 sq ft
Golf Course	457 E. McKinley – Golf Course Clubhouse 6,425 sq ft
	925 Pleasure Island Road – Golf Course Maintenance Shop 4,000 sq ft

PD Camera Locations:	
Beach	932 E. Silver Lake Road
Depot	116 S. Railroad Street
Riverview	203 E. Riverview Drive
Mural	128 S. Railroad Street
Rotary Square	229 E. Wall Street

Response to

CITY OF EAGLE RIVER Wisconsin

IT Managed Services Request for Proposal

Prepared by: Kevin McDaniel, CEO
IT Strategies Group, LLC
Date: September 2nd, 2025

601 Knightsbridge Road
Waunakee, WI 53597
it-strategies-group.com

Request For Proposal Transmittal

Date: October 19th, 2025

To: Robin Ginner, City Administrator- City of Eagle River
From: IT Strategies Group
Subject: Transmittal of Proposal for Information Technology Managed Services

---

Dear Robin & RFP Team at City of Eagle River,

On behalf of **IT Strategies Group**, I am pleased to submit our response to your Request for Proposal for Information Technology Managed Services.

Company Overview

IT Strategies Group is a trusted provider of managed IT services, consulting, and technology solutions. With a proven track record supporting organizations in **Healthcare, Financial Services, Municipal Government, and Manufacturing**, our mission is to deliver secure, reliable, and scalable IT solutions that enable our clients to focus on their core operations. We have successfully partnered with another municipal client whose IT environment closely mirrored the requirements outlined in your RFP. That client was also working with a one man IT shop prior to our engagement. This experience uniquely positions us to understand your current state and rapidly strengthen the security and stability of your environment.

Our team combines deep technical expertise with a customer-first approach, ensuring that each solution we implement is tailored to the specific needs of our clients. We provide proactive support, strategic guidance, and innovative solutions that drive efficiency and resilience.

Primary Contact Information

- **Firm Name:** IT Strategies Group
- **Contact:** Kevin McDaniel, President / CEO
- **Telephone:** (608) 665-9538
- **Email:** kevin.mcdaniel@it-strategies-group.com
- **Website:** www.it-strategies-group.com

We appreciate the opportunity to participate in this process and look forward to the possibility of working together. If you have any questions or need additional information, please do not hesitate to contact me directly.

Sincerely,
Kevin McDaniel
President
IT Strategies Group

Contents

Request For Proposal Transmittal i
The IT Strategies Group Approach ..... a
Support & Services Model ..... a
Staffing Levels ..... b
Support Diamond ..... b
Architecture & Account Management Team c
Security Operations Center Team (SOC Team) c
Systems Support Team c
Network Operations Center (NOC Team) ..... d
Onboarding Process & Timeline ..... d
Management of Weekly Workloads ..... g
After-Hours Contact & Support ..... g
IT Strategies Group's Team ..... h
Kevin McDaniel, CEO / President ..... h
Paul "Wally" Walton, Senior Field Support Engineer II (Level III Support) ..... h
Noah Gear, Service Delivery Engineer II (Level III Support) ..... h
Security Operations Center (SOC) i
Helpdesk Team i
Insurance ..... j
Examples of Work ..... k
Backup and Recovery Modernization ..... k
Security Policies / Program l
Security Policies l
Security Program l
Implemented a Centrally Managed Patching Management Solution ..... m
Hybrid Azure / On-Premises and Multi-Factor ..... o

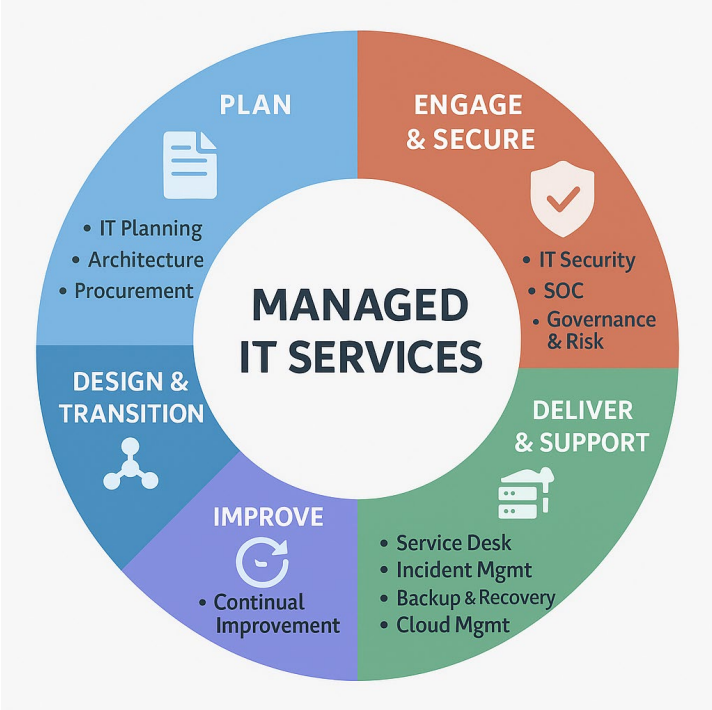
APPENDICIES....p
Services & Cost....p
Client's Preferred Cost Model....**Error! Bookmark not defined.**
Contract Year 2026 ....**Error! Bookmark not defined.**
Contract Year 2027 ....**Error! Bookmark not defined.**
One-Time Expenses: ....**Error! Bookmark not defined.**
IT Strategies Group's Costing Model ....p
Contract Year 2026 (Ongoing Expenses)....p
Contract Year 2027 (Ongoing Expenses)....q
One-Time Client Onboarding Fees .... r
Contract....s
Managed Services Agreement....s
Contract Schedules....ee
References....h
Response to CJIS Certification Requirement i

The IT Strategies Group Approach

Support & Services Model

IT Strategies Group's (ITSG) service delivery framework is based on the **ITIL model**, adapted specifically for the needs of small and medium-sized municipalities. While ITIL provides a robust and comprehensive framework, we have "right-sized" its application to ensure our clients receive **actionable insights and measurable value** without incurring unnecessary complexity or support costs. A key distinction in our approach is the prioritization of **"Engage & Secure"** as the second phase in the model, rather than the third as traditionally defined. This adjustment reflects our belief that client engagement and embedded security must be foundational to all IT operations, driving how we evolve an environment from its current state to a secure, optimized future state.

The diagram below illustrates our IT operations and support model as a **continuous circular process**, emphasizing that IT and security management are not static. Each iteration builds upon the last, enabling us to consistently address emerging operational requirements and evolving security threats while ensuring alignment with client goals.

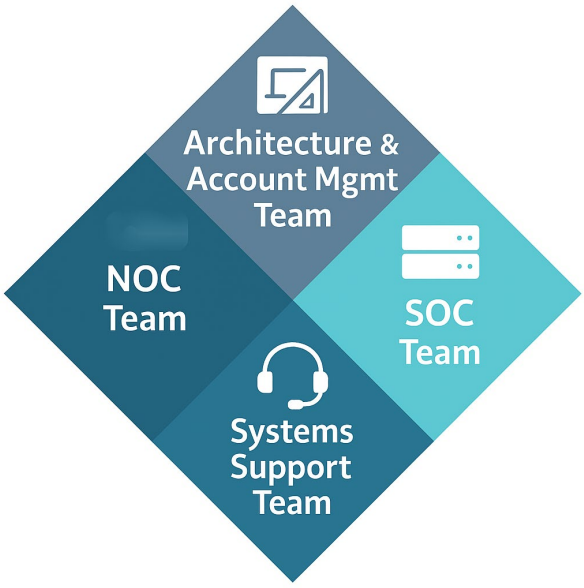


The following graphic extrapolates the model above down to our base focus in supporting our clients.

Staffing Levels

Support Diamond

The areas of focus and their associated tasks are broken up between the four teams in our IT Support Diamond, depicted below:



Architecture & Account Management Team

Each client is assigned a dedicated **Technical Account Manager (TAM)**, who is responsible for assessing and documenting the organization's **current IT state**—including operations, security, recoverability, and availability—and defining the **future state** required to meet organizational needs, regulatory obligations, and industry best practices. The TAM leads the development of the client's IT security program, oversees the creation of IT security policies, and produces a **three-year strategic roadmap** that details the initiatives needed to transition from current to future state. This roadmap provides a clear, forward-looking budget forecast, serves as a reference during quarterly business reviews, and supports annual budget planning through detailed project proposals.

In addition, the TAM, in collaboration with the NOC team, supports **third-party vendor management**, consults on new technologies and integrations, and provides **fractional CIO services**—ensuring each client benefits from strategic guidance as well as day-to-day operational oversight.

Security Operations Center Team (SOC Team)

Our Security Operations Center (SOC) is staffed with 20 full-time security professionals. Each client is supported by a **dedicated pod** of five SOC analysts who partner closely with the client's TAM, service delivery team, and field engineers to implement the IT security program. The SOC team continuously monitors telemetry from our security tools, analyzes potential threats, and ensures timely response to incidents. While their direct interaction with clients is limited compared to the systems support team, their work is central to **proactive threat detection, continuous monitoring, and the effective execution of the client's IT security strategy**.

Systems Support Team

ITSG's Help Desk is staffed by 15 full-time support professionals, organized into **pods of five personnel** dedicated to each client account. This structure ensures familiarity with the client's environment and consistent, personalized support. The Help Desk is available **24x7** and is the first point of contact for all service requests. When a ticket is opened, the Help Desk team will resolve the issue directly if it falls within their scope, with a target of resolving **80% of issues on the first call**. For issues requiring specialized expertise, the team triages and escalates the ticket to the appropriate support group to ensure timely resolution.

To maintain transparency and accountability, ITSG tracks a range of **service-level metrics**—including time-to-resolution and first-call resolution rates—and reviews these with each new client during onboarding. This ensures that the reporting aligns with the client's priorities and provides actionable data to measure the effectiveness of our support services.

Network Operations Center (NOC Team)

Each client is assigned two senior ITSG engineers who provide **third- and fourth-level support**, act as onsite resources when required, and serve as technical leads for IT-related projects. For this engagement, the designated senior staff are **Paul Walton** and **Noah Gear**, as listed in the *IT Strategies Group's Team* section of this proposal.

Both the **Systems Support** and **Network Operations Center (NOC)** teams operate within the *Deliver & Support* segment of our Managed IT Services model. The Systems Support team also partners with the **Security Operations Center (SOC)** team to remediate identified security issues and implement security solutions, ensuring operational and security objectives are achieved in tandem. In addition, the NOC team collaborates closely with the Technical Account Manager (TAM) to support the *Improve* and *Design & Transition* phases, ensuring that operations, projects, and long-term strategies remain aligned and continuously optimized.

Together, this **cross-team collaboration**—between Systems Support, SOC, NOC, and TAMs—embodies our ITIL-based *continuous improvement cycle* and aligns directly with the **ISO/IEC 27001 Plan–Do–Check–Act (PDCA) model**. This ensures client environments are not only well-supported and secure but are also continuously assessed, improved, and adapted to meet evolving operational, regulatory, and cybersecurity requirements.

Onboarding Process & Timeline

Here is a visual representation of our onboarding process:

In the onboarding process listed below, we ask to start Phase 1 two (2) to three (3) weeks prior to taking over the environment. Regarding Eagle River's request for your new managed services provider to take over on January 1st, this would have us start the onboarding the first or second week of December. We can, and have, started onboarding the same day as cut over, it just slows down our initial impact on your environment by a week or two.

Phase 1 – Discovery & Planning (Week 1–2)

- Conduct kickoff meeting with client leadership and key stakeholders.
- Collect and review IT documentation (network diagrams, asset inventory, vendor contracts, licensing, compliance requirements).
- Perform security and infrastructure assessments (active directory, endpoints, servers, cloud platforms, backups).

- Define service-level expectations and success criteria.
- Establish communication channels and escalation procedures.
- Start planning the police department's migration to an in-house replacement for their document management / DOJ records access service from Vilas county.

Phase 2 – Access & Environment Setup (Week 2–3) (In case of no early access to environment, this would be combined with Phase 1)

- Configure client in MSP systems (ticketing, RMM, SOC, monitoring dashboards).
- Establish secure administrative access to client infrastructure.
- Deploy agents for monitoring, patch management, and endpoint protection.
- Configure backup validation and reporting.
- Document all credentials, integrations, and dependencies in secure vaults.

Phase 3 – Policy & Security Alignment (Week 3–4)

- Develop or update IT security policies (aligned to ISO 27001/NIST standards).
- Implement multi-factor authentication (MFA), conditional access, and password policies.
- Align backup/recovery processes with RPO/RTO requirements.
- Establish change management and incident response procedures.
- Start user awareness training on security and support processes.

Phase 4 – Stabilization & Optimization (Month 2–3)

- Review performance of monitoring, patching, and security systems.
- Address gaps identified in assessments (e.g., unsupported software, unpatched systems).
- Create, review, gain approval for and implement prioritized roadmap.
- Conduct quarterly business review (QBR) to validate alignment with client goals and compliance obligations.

Phase 5 – Continuous Improvement (Ongoing)

- Quarterly security and operational reviews with client leadership.
- Annual risk assessment and policy updates.
- Ongoing refinement of IT roadmap to align with regulatory changes, business needs, and emerging threats.
- Regular recovery testing and reporting to ensure business continuity.

⏱️ **Typical Timeline:**

- Initial discovery and setup: **30–45 days**
- Stabilization and optimization: **60–90 days**
- Continuous improvement: **Quarterly & annual cycles**

✅ **Best Practice Alignment:**

- **ISO/IEC 27001:** Plan–Do–Check–Act model for governance.
- **ITIL:** Service transition, change management, and continual service improvement.
- **NIST:** Security controls for patching, access, incident response, and recovery.

Management of Weekly Workloads

The workload of our **SOC** and **Systems Support** teams are staffed to comfortably handle projected call volumes based on the size and types of clients we support. Both teams also maintain additional resources that can be reassigned to client pods as needed, ensuring responsiveness even during periods of higher-than-expected demand.

For the **NOC team**, industry best practice is that each technician supports up to **500 workstations** (with an assumed ratio of five servers per 100 workstations and up to 10 sites). ITSG adopts a more conservative model, assigning no more than **350 workstations per technician** while maintaining the same server and site assumptions. Currently, senior engineers **Paul Walton** and **Noah Gear** are each supporting fewer than **200 workstations**, meaning the addition of your account remains well within our thresholds.

We continuously evaluate projected growth and the impact on supported device metrics, proactively hiring and onboarding new staff ahead of demand. This disciplined approach ensures we maintain the staffing capacity necessary to deliver **consistent, world-class support** to all clients.

After-Hours Contact & Support

Client staff can open service tickets through our **ticketing portal** or by contacting the **Help Desk** directly. For emergencies requiring a response within 30 minutes or less, clients are instructed to call the Help Desk to ensure immediate attention. **After-hours support** is available for critical emergencies only (as defined in the Contract Schedules), and in such cases, the Help Desk will either resolve the issue or escalate it directly to the NOC team. Senior leadership at all client organizations are also provided with direct contact information for their TAAM and **Kevin McDaniel, President of ITSG**, as an additional escalation path when necessary.

The **SOC team** provides 24x7 monitoring of security events. If a critical security incident is detected, the SOC will engage the NOC team's on-call resource immediately. Once the NOC confirms the event as a valid threat, they will promptly contact the client's designated primary IT contact to inform them of the situation and initiate the appropriate response steps.

IT Strategies Group's Team

Kevin McDaniel, CEO / President

Kevin McDaniel is a seasoned IT leader with over 25 years of experience helping municipalities and companies strengthen their technology environments, reduce costs, and safeguard critical services. As President of IT Strategies Group, he has guided government clients through disaster recovery efforts, enabling over 600 organizations to restore systems after cyber incidents or natural disasters, while consistently negotiating IT investments that deliver 30%+ savings. With deep expertise in IT security, infrastructure, and enterprise architecture, Kevin bridges the gap between technical teams and city leadership, ensuring technology decisions are aligned with fiscal responsibility, compliance requirements, and the reliable delivery of citizen services.

Kevin has the following certifications: TOGAF Architect, MSCE, ISO27001 & is completing his CISM classification by end of year 2025

Paul "Wally" Walton, Senior Field Support Engineer II (Level III Support & TAAM)

Paul Walton is an experienced IT leader with over 20 years managing large-scale technology operations, including 13 sites and 9,000 endpoints for the Middleton-Cross Plains Area School District. He specializes in strengthening security, streamlining IT services to ITIL standards, and leading multi-vendor projects that deliver measurable cost savings and improved reliability. Paul brings municipalities proven expertise in modernizing IT environments to ensure secure, efficient, and dependable services for staff and citizens.

Paul has the following certifications: A+, MCP Win95 through Win7, MS SharePoint Admin, MS Exchange Admin, MS Server Admin, Apple Certified Support

Noah Gear, Service Delivery Engineer II (Level III Support)

Noah Gear is an IT professional with experience leading a 12-person helpdesk team at Cognizant supporting Meta, where he managed ticket workflows, SLA compliance, and end-user support across Windows, Mac, Linux, iOS, Android, and ChromeOS environments. He has hands-on expertise with cloud storage platforms (Google Drive, OneDrive, Dropbox), system administration, security software, and incident management under ITIL standards. Noah's role included acting as SME for operating system and software troubleshooting, creating SOPs and runbooks, optimizing service desk operations, and using data analysis tools like Tableau to monitor and improve team performance—experience directly relevant to delivering reliable and efficient IT managed services.

Noah has the following certifications: Datto RITSM and is working on his CompTIA+ and A+ certifications

Security Operations Center (SOC)

Our Managed Services Security Operations Team (SOC) provides 24/7 monitoring, detection, and incident response to protect client environments across healthcare, financial, municipal, and manufacturing industries. The team consists of SOC managers, tiered security analysts, incident response specialists, compliance analysts, and threat intelligence experts who leverage SIEM, SOAR, and threat intelligence platforms to deliver proactive defense, compliance, and rapid remediation. With certifications including CISSP, CISM, Security+, CySA+, CEH, OSCP, GIAC, ISO 27001, CISA, HCISPP, and cloud security credentials from Microsoft, AWS, and Google, the team ensures comprehensive coverage in operations, forensics, threat hunting, compliance, and cloud security, aligning services with frameworks such as NIST, ISO 27001, and CIS Controls.

Helpdesk Team

Our Tier 1 and Tier 2 support teams provide **round-the-clock, 24/7 technical assistance** to ensure uninterrupted service for our clients. **Level 1 agents** are trained to deliver rapid response and resolve common issues quickly, while **Level 2 engineers** handle more complex incidents and escalations with advanced expertise. Each member of our help desk team is highly qualified, holding a combination of **CompTIA, ITIL, and HDI certifications**, which ensures both technical proficiency and strict adherence to IT service management best practices. For municipalities in particular, we deliver measurable value by **guaranteeing live support within two minutes of every call**. This commitment minimizes downtime for critical public services and enables local governments to operate with the **efficiency, reliability, and professionalism** their communities depend on.

Insurance

The insurance coverage that we have is also provided in the Managed Services Agreement “MSA”, a copy of which is provided in the “Contract” section of our response.

Business Owners General Liability Insurance

- $1,000,000 liability and medical expenses
- $10,000 medical expenses (per person)
- $300,000 damages to rented property

Technology Professional Services (errors and omissions)

- $1,000,000 each claim

Umbrella Coverage (aggregates base policies above)

- $1,000,000

Examples of Work

Work examples specific to our work with municipalities are listed below. Examples of the work product (design documents, etc.), will be happily provided if selected as a finalist.

Backup and Recovery Modernization

When we assumed responsibility for this client's IT environment, their backup strategy relied on a dual solution of iDrive and Windows Server Backup. This approach created several critical risks: conflicting backup processes, no integrity validation, no reporting on failures, no recovery testing, no documented recovery plan, and no integration with the client's overall IT security program. Collectively, these gaps left the client unable to guarantee recovery point (RPO) or recovery time objectives (RTO).

We implemented our standardized backup and recovery solution to address these issues and provide a secure, validated, and reliable framework:

Validated Redundancy – All servers back up to a local appliance, where backups are validated, then replicated and re-validated in the cloud.

Rapid Recovery – Failed servers can be restored locally within 30 minutes; in a site-wide disaster, all servers can be brought online in the cloud within two hours (far exceeding the client's 72-hour RTO).

Granular Protection – Hourly incremental backups between 7 AM and 4 PM ensure a maximum 24-hour data loss window, fully meeting the client's RPO.

Proactive Oversight – Daily monitoring alerts and TAM-reviewed reports ensure immediate remediation of backup issues.

Annual Recovery Testing – Virtualization makes it easy to test and confirm recovery processes annually.

Security Integration – Backup and recovery are fully tied into the client's IT security program, ensuring alignment with compliance and resilience requirements.

This solution not only eliminates the risks of the legacy environment but also **exceeds the client's stated RPO (Recovery Point Objective) and RTO (Recovery Time Objective) requirements**, delivering confidence that business-critical systems and data are recoverable under any circumstance.

Security Policies / Program

Security Policies

When we assumed management of the client's IT environment, we found they lacked formal IT security policies, the foundation of any effective information security program. Recognizing that policies set the organizational tone, define accountability, and establish consequences for noncompliance, we provided templates for our standard set of thirteen core IT security policies. We then collaborated with the municipality to tailor these policies to their specific environment, accelerating adoption while ensuring alignment with applicable regulatory frameworks such as CJIS, as well as the client's cyber insurance requirements.

This approach not only reduced implementation time but also established a governance framework consistent with **ISO/IEC 27001 best practices**, including risk management, access control, incident response, and business continuity. By embedding security policy into daily operations, the municipality gained a defensible posture against audits, improved compliance readiness, and a clear roadmap for continuous security improvement.

Security Program

Once the IT security policies were established, we built a comprehensive IT security program to operationalize them. This program translated policy into actionable procedures and measurable controls, enabling compliance to be monitored, demonstrated, and continuously improved through corrective action when necessary. At its core, the program provided the client with a structured process to conduct annual risk assessments addressing both internal and external threats, prioritize remediation efforts, and track progress against documented security objectives.

The program also established a formal **change management system**, aligned with ISO/IEC 27001 requirements, ensuring that all modifications to the IT environment were reviewed, approved, or rejected by the client's leadership team based on risk impact, security posture, and timing considerations. In addition, the program incorporated key ISO 27001 elements such as **incident response planning**, **business continuity and disaster recovery integration**, and a **cycle of continuous improvement (Plan–Do–Check–Act)** to strengthen resilience over time. This governance model enhanced transparency, accountability, and alignment with regulatory and insurance obligations.

This framework positioned the client to demonstrate compliance with recognized standards, reduce security risk, and provide leadership with confidence that the organization's IT environment is both well-governed and audit ready.

Implemented a Centrally Managed Patching Management Solution

The IT services provider that preceded us at this client was using Microsoft Update Service to patch their servers and endpoints (workstations / laptops). While this process is better than no process, it doesn't meet the following patch management best practices (as outlined in the ISO27001, NIST SP 800-40 and CIS benchmarks):

Limited Vendor Application Coverage- Microsoft update service only covers Microsoft products. Best practice requires patching across the entire IT environment (hardware and software). From a hardware perspective it doesn't provide coverage for other operating systems, nor networking and network attached storage equipment). Regarding software, it does not cover third-party application patching such as frequently used applications like Adobe, Java, Browsers, Line-of-Business Software, firmware, etc… All of which are frequent attack vectors.

Inadequate Testing & Staging Capabilities- While Windows update service can delay or approve updates, it lacks robust sandboxing / staging environments. Best practices call for structured test-approve-deploy cycle to reduce the risk of downtime or incompatibility.

Limited Reporting & Compliance Verification- Reporting in Windows update service is minimal and often unreliable. ISO27001 and NIST recommend organizations be able to demonstrate compliance with patching requirements (who was patched, when, and whether it succeeded). Microsoft update service does not provide this dashboard / reporting.

No Automated Remediation or Enforcement- If a patch fails to apply, Windows update service doesn't automatically reattempt or remediate. Best practice requires mechanisms to detect, retry and confirm patch deployment.

No Integration with Risk Management- Patching should be based on severity, exploitability, and asset criticality. Windows update service applies Microsoft's schedule (Patch Tuesday, occasionally out of band), it is not tailored to organizational risk-based prioritization.

Limited Change Management & Approvals- Windows update service lacks built in workflows to integrate with ITIL or ISO27001change management processes. Best practice requires documenting approval, scheduling and rollback plans for patches.

No Coverage for Offline or Remote Devices- Devices that are mobile, offline, or outside the corporate network may not consistently receive patches. Best practices require centralized control and reporting for all endpoints, wherever they are.

We implemented our integrated tools impacting patch management (remote monitoring and management, ticketing system and documentation). The implementation of these tools corrects the deficiencies inherent (and listed above) by using only Microsoft update service.

Hybrid Azure / On-Premises and Multi-Factor

A client that we onboarded was using both Microsoft 365 (MS Office / Azure (now Entra)), and utilized on-premises active directory servers to authenticate and manage access to their on-premises IT environment. Relying solely on on-premises Active Directory without an Entra ID (Azure AD) hybrid integration and Duo multi-factor authentication (MFA) does not meet ISO/IEC 27001 or NIST security requirements because it fails to enforce modern identity and access management controls. Best practices under both frameworks require strong authentication, centralized identity governance, conditional access, and secure federation for cloud services. Without a hybrid identity model, organizations lack unified visibility and control over user accounts across cloud and on-prem systems, increasing the risk of credential compromise and unauthorized access. Likewise, without MFA, the environment violates explicit requirements for strong authentication (ISO 27001 Annex A.9, NIST 800-63B), leaving critical systems dependent on single-factor passwords, which are inadequate against phishing and brute-force attacks.

To ensure that our client had maximum protection, we instituted an Azure Hybrid model, which provided single sign on between their system login and M365 login. It also provided the most secure model in which to implement multi-factor authentication through rolling out Cisco's Duo product.

APPENDICIES

Services & Cost

IT Strategies Group's Costing Model

Contract Year 2026 (Ongoing Expenses)

Device Type	# Devices	Standard Cost / Device / Month	Standard Extended Cost / Month	Municipality Discount / Device / Month	Total Net Monthly Cost
Endpoints	18	$139	$2,502	$47.68	$1,644
Servers	1	$139	$139	$47.68	$91
Firewall Mgt	3	$77	$231	$10	$201
Storage (NAS)	0	$77	$0	$10	$0
Printers	3	$25	$75	$5	$60
Sites	3	$100	$300	$15	$240
Phones	40	$25	$1,000	$0	$1,000
		Total	**$4,247**	**Total**	**$3,236**

*NOTE: We assumed one large, shared printer per site and will adjust upon further information.

*NOTE: We took average cost / line for phones ($23.50 to $31) as we do not know if you need MS Teams integration, or other advanced features. We also did not include new phone devices. We do offer phone leasing and purchase options.

Contract Year 2027 (Ongoing Expenses)

Device Type	# Devices	Standard Cost / Device / Month	Standard Extended Cost / Month	Municipality Discount / Device / Month	Total Net Monthly Cost
Workstations	18	$146	$2,628	$50	$1,728
Servers	1	$146	$146	$50	$94
Firewall Mgt	3	$81	$243	$11	$210
Storage (NAS)	0	$81	$0	$11	$0
Printers	3	$26	$78	$5	$63
Sites	3	$105	$315	$16	$267
Phones	40	$26	$1,040	$0	$1,040
		Total	**$14,771**	**Total**	**$3,402**

*NOTE: We assumed one large, shared printer per site and will adjust upon further information.

NOTE: We assumed no growth in environment, if number of devices change, costs will change relative to that device type's charge per month.

NOTE: We did assume a annual increase per contract of 5% (or cost of inflation, whichever is higher)

Contract Year 2027 (Ongoing Expenses)

Device Type	# Devices	Standard Cost / Device / Month	Standard Extended Cost / Month	Municipality Discount / Device / Month	Total Net Monthly Cost
Workstations	18	$153	$2,754	$51	$1,836
Servers	1	$153	$153	$51	$102
Firewall Mgt	3	$85	$243	$11	$222
Storage (NAS)	0	$85	$0	$11	$0
Printers	3	$27	$81	$5	$66
Sites	3	$110	$330	$16	$282
Phones	40	$27	$1,080	$0	$1,080
		Total	**$14,771**	**Total**	**$3,588**

*NOTE: We assumed one large, shared printer per site and will adjust upon further information.

NOTE: We assumed no growth in environment, if number of devices change, costs will change relative to that device type's charge per month.

NOTE: We did assume an annual increase per contract of 5% (or cost of inflation, whichever is higher)

One-Time Client Onboarding Fees

On-Boarding Fees	**$3,236**

NOTE: Onboarding fee is equal to one month's service fees.

Example Contract

Managed Services Agreement

SERVICES AGREEMENT

BETWEEN

IT STRATEGIES GROUP, LLC AND

XXXX

This Services Agreement (the "Agreement") is made and entered into on MONTH, DAY, YEAR by and between the XXXX ("Client") and IT Strategies Group, LLC ("Contractor").

1. SERVICES. During the Term of this Agreement (defined in Section 3.C.), Contractor shall provide Client with the Managed IT Services ("Services") set forth on the attached Schedule A and, if requested and agreed to by Contractor and Client in a separate statement of work, the "Excluded Services" set forth on the attached Schedule B. For avoidance of doubt:

A. Schedule A – Service Offering summarizes the categories of services Client requested as part of its Request for Proposal, and Contractor shall provide the Services contained in Schedule A.

B. Appendix A to Schedule A identifies the response times and levels of support to be provided by Contractor pursuant to the Services.

C. Appendix B to Schedule A provides further detail on how Contactor shall provide the Services.

2. DUTIES OF THE PARTIES.

A. Duties of Contractor: Contractor agrees to use commercially reasonable efforts to timely deliver and support the Services for Client in accordance with industry standards.

B. Duties of Client: Client agrees to:

(1) Timely submit all payments to Contractor at Contractor's place of business.

(2) Provide Contractor with access to Client's facilities, including access to Client's computer systems, according to Client's procedures, which procedures shall be provided to Contractor in writing and in advance of the Services.

(3) Provide adequate and suitable facilities and space for Contractor's personnel to work at Client's facility (as needed) and on such computer systems.

(4) If Contractor determines that the Services require Contractor to remotely access Client's computer systems, Client agrees that it shall also provide Contractor with all the information reasonably requested by Contractor for Contractor to remotely access Client's computer systems.

(5) Client also acknowledges and agrees that the providing of the Services by Contractor may in some circumstances result in the disruption of services at Client's facility or on Client's computer systems, or loss or damage to software or hardware. Although Contractor shall take reasonable steps consistent with industry standards to avoid the disruptions, losses, and damages described in the preceding sentence, Contractor cannot guarantee that Client will not incur such disruptions, losses, or damages.

3. PRICING, PAYMENT AND TERM / TERMINATION.

A. Fees:

The fees ("Fees") for Services are set forth on the attached Schedule C. To the extent Client and Contractor agree that Contractor shall perform Excluded Services as set forth in Schedule B pursuant to a separate statement of work, the fees for Excluded Services are identified in Schedule

B. Payment:

(1) Contractor shall invoice Client on a monthly basis for Services to be performed. Contractor shall invoice Client on a quarterly basis for tools Payments shall be made via check or ACH. Client shall pay Contractor within thirty (30) days of receiving the invoice. All hardware / software orders must be pre-paid, with invoice due upon receipt.

(2) To the extent Client and Contractor agree that Contractor shall perform Excluded Services as set forth in Schedule B, Client shall pay Contractor within thirty (30) days of receiving the invoice for the Excluded Services. All hardware / software orders must be pre-paid, with invoice due upon receipt.

(3) Contractor shall have no obligation to perform Services or Excluded Services for Client unless all invoices are paid in full on a timely basis. In the event of nonpayment of any sum due and owing under this Agreement, Contractor shall have the right to suspend or immediately terminate the provision of Services or Excluded Services.

(4) Any payment not received by Contractor within thirty (30) days of the Client's receipt of the invoice shall bear interest from the due date until paid in full at the lesser of one and percent (1.5%) per month or the maximum rate allowed by applicable law.

(5) During the term of this agreement and to the extent this Agreement is extended beyond the Term defined in Section 3C., Fees are subject to an increase of up to five (5) percent per year or the annual rate of inflation (as set by the Federal Reserve), whichever is higher.

C. Term and Termination:

(1) This Agreement shall be effective for two (2) years, with Services commencing on January 1, 2026 ("Effective Date"), and shall automatically renew for additional one-year periods on each anniversary of the Effective Date if notice to end contract by either party is not received 90 days prior, or unless terminated under this Section 3.C. The initial three-year period and each one-year period of this Agreement (or such shorter or longer period of effectiveness as mutually agreed to by Contractor and Client) is referred to as an "Effective Period" and collectively all of the Effective Periods of this Agreement are referred to as the "Term."

(2) Either party may terminate this Agreement at any time by providing at least three (3) months' prior written notice to the other party ("Notice Period"). Client acknowledges and agrees that Client is responsible for paying monthly Fees during the Notice Period, regardless, if Client requests not to receive Services during the Notice Period, at the same monthly amount as the average of the three (3) month period immediately preceding the notice of termination. Client also remains responsible for all hardware / software lease and / or licensing payments for the remainder associated with their terms (regardless of termination of services).

(3) Contractor may immediately terminate this Agreement upon written notice to Client if Client (i) fails to make any payment to Contractor when due and such failure continues for a period of five (5) business days following written notice of such failure by Contractor to Client; or (ii) breaches any other provision of this Agreement. Client may immediately terminate this Agreement upon written notice to Contractor if Contractor breaches any provision of this Agreement.

(4) Immediately upon the expiration or termination of this Agreement, Client and Contractor shall (i) return to each other any and all equipment provided by the other party; and (ii) discontinue the use of and permanently delete from the party's computer systems any and all of the other party's software and computer programs.

4. OWNERSHIP. All materials, including all copyrights, trademarks, logos, and other identifying marks (collectively "Materials") of each party are and shall remain the exclusive property of that party, and except as otherwise specifically set forth in this Agreement, no license to use such Materials is granted pursuant to this Agreement. All Materials are proprietary and may not be reproduced, duplicated or disseminated for any purpose. All non-third-party software installed or provided by one of the parties for the other party's use is proprietary software and the exclusive property of installing party.

5. CONFIDENTIAL INFORMATION.

A. Pursuant to the provision of Services under this Agreement, either party may gain access to the other party's Confidential Information. Each party will adopt commercially reasonable measures to protect the other party's Confidential Information provided pursuant to this Agreement, subject to the Wisconsin Public Records Law, Wis. Stat. §§ 19.21 – 19.39, or any corresponding federal laws.

B. For purposes of this Agreement, "Confidential Information" means:

(1) Any inventions, processes, designs, trade secrets, formulas and formulations, methods and methodologies, know-how, samples, tests, technologies, diagrams and flowcharts, standard and non-standard operating procedures and other data;

(2) Any financial information (including but not limited to price lists, quotes, estimates, and rates), results of consultancies, contracts, customer lists and relationships, and other information which may be needed to be disclosed by each party to the other in relation to business negotiations or operations in whatever form (written, oral, visual, electronic); and

(3) All other information that one of the parties reasonably identifies as confidential.

C. For purposes of this Agreement, "Confidential Information" does not include information which:

(1) The recipient can demonstrate in writing to be rightfully known to recipient at the time it receives the information;

(2) Has become publicly known through no wrongful act of the recipient;

(3) The recipient can demonstrate in writing to have been rightfully received by recipient from a third party authorized to make such communication without restriction; or

(4) Has been approved for release by written authorization of the discloser.

D. Subject to the Wisconsin Public Records Law or any corresponding federal laws, each party undertakes to hold any and all Confidential Information in confidence and to use it exclusively for the purposes set forth in this Agreement. Neither party shall, directly or indirectly, make use of the Confidential Information of the other party without the other party's prior, written consent.

E. Client agrees that it will promptly notify Contractor in writing if Client receives a request under the Wisconsin Public Records Law or any corresponding federal laws seeking disclosure of any part of the Confidential Information. Client shall not disclose any part of the Confidential Information for a period of ten (10) business days after giving written notice to Contractor. Within ten (10) business days of Client giving such written notice, Contractor shall notify Client in writing of whether or not the Confidential Information can be released.

(1) If Contractor fails to notify Client in writing within such ten (10) business day period, Client may release the Confidential Information.

(2) If Contractor notifies Client in writing within such ten (10) business day period that the Confidential Information may be released, the Confidential Information may be released.

(3) If Contractor notifies Client in writing within such ten (10) business day period that the Confidential Information may not be released then:

(i) If Client's attorney concurs that such Confidential Information is not subject to release under the Wisconsin Public Records Law or any corresponding federal laws, Client shall refuse to release the Confidential Information and Contractor shall reimburse Client for any reasonable attorney fees incurred by Client in contesting the request for Confidential Information, including all costs associated with litigation and any penalties or other attorney fees due under Wis. Stat. § 19.37.

(ii) If Client's attorney does not concur that such Confidential Information is not subject to release under the Wisconsin Public Records Law or any corresponding federal laws, Client shall give Contractor ten (10) days' written notice to enable Contractor to commence an action for a protective order. If Contractor fails to commence an action for a protective order within said ten (10) day period, Client may release such Confidential Information. If Contractor commences an action for a protective order within said ten (10) day period, Client shall not release the Confidential Information until and unless there is a final non-appealable order on Contractor's action for a protective order that requires the release of the Confidential Information. To the extent that Client incurs legal fees related to Contractor's action for a protective order or an action contesting the request for Confidential Information after Client's attorney does not concur with Contractor's determinations, Contractor shall reimburse Client for any reasonable attorney fees incurred by Client, including all costs associated with litigation and any penalties or other attorney fees due under Wis. Stat. § 19.37.

F. In addition to Section 5.E. above, a recipient may disclose Confidential Information if required by court or government action to be disclosed; provided, however, the recipient must first provide the discloser with reasonable prior, written notice of such disclosure so that the discloser may attempt to prevent such disclosure, and that the Confidential Information shall continue to be treated as Confidential Information for all other purposes.

6. HIRING OF CONTRACTOR EMPLOYEES. In the absence of Contractor's prior written consent, and for a period of twelve (12) months following the expiration or termination of this Agreement, for any reason whatsoever, Client agrees not to hire or engage, directly or indirectly, any person who, at any time during the twelve (12) months immediately preceding such hiring or engagement, was an employee of Contractor who performed Services, Excluded Services, or similar services for Contractor for any customer of Contractor. Contractor and Client agree that the damages from a breach of this Section 6 would be difficult to ascertain. Therefore, in the event Client breaches this Section 6, Client shall pay Contractor, as liquidated damages and not as a penalty, a sum equal to twenty-four (24) months' pay for each former employee of Contractor hired by Client, at the rate paid by Contractor for the last full month of such employee's employment with Contractor. In addition, Contractor shall be entitled to temporary and permanent injunctions in order to prevent or restrain any such violation of this Section 6 by Client. These remedies shall be in addition to, and not in limitation of, any other rights or remedies afforded to Contractor under this Agreement or available to Contractor at law or in equity.

7. FORCE MAJEURE. Except for payment obligations, the parties shall not be responsible for failure to render any obligation due to causes beyond their reasonable control, including, but not limited to, work stoppages, fires, civil disobedience, riots, rebellions, floods, war, acts of terrorism, delays in transportation, accident, failure of Client to provide a suitable operating environment for Contractor, hardware malfunctions caused by defects in software or otherwise, failure of Client to allow Contractor access to its computer system, acts of God, and other similar occurrences. The obligations and rights of the parties shall be extended on a day-to-day basis for the duration of excusable delay.

8. REPRESENTATIONS AND WARRANTIES. Each party represents and warrants to the other party that (i) it has the full right, power and authority to enter into and to perform this Agreement; (ii) the execution, delivery and performance of this Agreement has been duly authorized by all necessary corporate / organizational action; (iii) this Agreement constitutes a valid and binding obligation of such party, enforceable against it in accordance with its terms, subject to applicable bankruptcy, insolvency, reorganization, moratorium and other laws affecting the rights of creditors generally; and (iv) the execution, delivery and performance of this Agreement does not or will not violate or cause a breach or default under (a) the governing corporate or company documents of such party; (b) any agreement, lease, mortgage, license or other contract to which such party is a party; or (c) any law, rule, regulation, order, decree or consent action by which such party is bound or to which it is subject.

9. DISCLAIMER OF WARRANTIES. CONTRACTOR DOES NOT WARRANT THE UNINTERRUPTED OR ERROR-FREE OPERATION OR PROVISION OF THE SERVICES, THAT THE SERVICES WILL BE FREE FROM INTERRUPTION, THE SERVICES WILL BE SECURE FROM UNAUTHORIZED ACCESS, THAT THE SERVICES WILL DETECT EVERY SECURITY OR OTHER VULNERABILITY OF CLIENT'S COMPUTER SYSTEMS, OR THAT RESULTS GENERATED BY THE SERVICES WILL BE ERROR-FREE, ACCURATE OR COMPLETE. ALL INFORMATION, MATERIALS AND SERVICES ARE PROVIDED TO CLIENT "AS IS". EXCEPT AS SPECIFICALLY SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

The Services may become unavailable due to any number of factors, including, without limitation, scheduled or unscheduled maintenance, technical failure of the software, telecommunications infrastructure, or the availability or interruption of access to the Internet. The disclaimers set forth in this Section shall apply regardless of whether (i) Contractor determines that Client's computer systems are deemed "secure", (ii) Client performs such modifications to its computer systems as Contractor reasonably suggests in order for Client's computer systems to be deemed "secure", or (iii) otherwise.

10. INSURANCE. Contractor shall maintain the following insurance coverage and shall name Client as a co-insured:

Business Owners General Liability Insurance

- $1,000,000 liability and medical expense
- $10,000 medical expense (per person)
- $300,000 damages to rented property

Technology Professional Services (errors and omissions)

- $1,000,000 each claim

Umbrella Coverage (aggregates base policies above)

- $1,000,000

11.

A. LIMITATION OF LIABILITY. CONTRACTOR SHALL NOT BE LIABLE TO ANY THIRD PARTY FOR ANY OF THE FOLLOWING ARISING OUT OF THIS AGREEMENT AND/OR THE SERVICES: ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, WHETHER BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT TORT OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT CONTRACTOR IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR ANY LOSS OF PROFITS, LOSS OF DATA, EQUIPMENT DOWNTIME, OR LOSS OF GOODWILL.

B. CLIENT ACKNOWLEDGES AND AGREES THAT CONTRACTOR'S AGGREGATE LIABILITY TO CLIENT FOR ANY DAMAGES, LOSSES, FEES, CHARGES, EXPENSES AND/OR LIABILITIES ARISING OUT OF WITH THIS AGREEMENT AND/OR THE SERVICES SHALL NOT EXCEED THE INSURANCE LIMITS AS PROVIDED IN SECTION 10 ABOVE.

C. Client acknowledges that the limitations on liability were specifically bargained for and are acceptable to Client. Client's willingness to agree to the limitations of liability set forth in this Section was material to Contractor's decision to enter into this Agreement. The limitations on liability set forth in this Section shall be enforceable to the maximum extent permitted by applicable law.

12. GENERAL TERMS.

A. This Agreement is the entire agreement between Contractor and Client and supersedes any prior understandings or written or oral agreements between Contractor and Client with respect to the subject matter of this Agreement.

B. This Agreement may only be amended or changed pursuant to a written document duly executed by both Contractor and Client.

C. No waiver of a breach of any provision of this Agreement by any party shall be construed as a waiver of a subsequent breach of the same or any other provision of this Agreement.

D. Client's obligation to pay for any Services or other services received by Contractor, and each of the provisions of Section 3, 5 through 8, and 10 through 15 shall survive the expiration or earlier termination of this Agreement.

E. The invalidity of any provision of this Agreement shall not affect the enforceability of the remaining Agreement or any other provision of the Agreement.

F. All Schedules to this Agreement are true, correct and hereby incorporated into by reference and made a part of this Agreement.

G. This Agreement shall be binding upon, inure to the benefit of, and be enforceable by Contractor and Client and their successors and permitted assigns, and no other person or entity shall have or acquire any right by virtue of this Agreement unless otherwise specifically agreed to in writing by Contractor and Client.

H. This Agreement and the rights and obligations of the parties are not assignable without the prior written consent of the other party. Any attempt by one of the parties to assign any this Agreement or any right, duty, or obligation which arises under this Agreement, without such consent, will be void.

I. This Agreement shall not be construed to give any person other than Contractor and the Client any legal or equitable right, remedy or claim under or with respect to this Agreement. This Agreement shall not create a joint venture, partnership or other formal business relationship or entity of any kind, or an obligation to form any such relationship or entity. Each party will act as an independent entity and not as an agent of the other party for any purpose, and neither will have the authority to bind the other.

J. This Agreement may be executed in multiple counterparts, each of which shall be deemed to be an original and of equal force and effect, and all of which taken together shall constitute one and the same instrument.

K. The parties reserve the right to maintain an executed copy of this Agreement in electronic form only and agree that a print-out of such electronic form of this Agreement will be deemed an original for all purposes relating to the enforceability of the terms and conditions of this Agreement.

13. NOTICES. All notices required pursuant to this Agreement shall be written and shall be delivered by (i) hand-delivery; (ii) nationally recognized overnight delivery service (such as FedEx, UPS, DHL, or USPS Express Mail); or (iii) electronic mail with verification of receipt. All such notices and other communications shall be addressed to the other party at the address set forth in this Agreement or to such other address as a party may designate by notice complying with the terms of this Section. Each such notice shall be deemed delivered (i) on the date delivered if by hand-delivery; (ii) on the date delivered or the date delivery is refused by the recipient, if by nationally recognized overnight delivery service; or (iii) upon verification of receipt if by electronic mail.

14. DISPUTE RESOLUTION. Except as otherwise specifically set forth in this Agreement, the parties hereby agree to resolve any and all controversies, claims and/or disputes arising out of this Agreement and/or any Services (each, a "Dispute") solely pursuant to the terms of this Section.

A. Management Resolution. All Disputes shall first be referred to the parties' authorized representatives for discussion and resolution of the Dispute ("Management Resolution"), which representatives are the individuals who have executed this Agreement on behalf of their party, or his or her designee.

B. Arbitration. If Management Resolution fails to resolve the Dispute, then the Dispute shall be resolved by final, binding arbitration ("Arbitration") in Madison, WI administered by the American Arbitration Association ("AAA") under the AAA's Commercial Arbitration Rules.

C. Governing Law; Venue; Jurisdiction. This Agreement shall be governed by, and construed in accordance with, the laws of the State of Wisconsin (without giving effect to principles of conflicts of laws). For any action to compel Arbitration, enforce an Arbitration award or seek injunctive relief pursuant to this Agreement, the parties hereby expressly consent to the (i) venue of Dane County, Wisconsin, USA, and each party hereby expressly waives any objection to such venue based upon forum non-convenient or otherwise; and (ii) jurisdiction of the state and/or federal courts in and/or for Dane County, Wisconsin, USA.

D. Prevailing Party Attorney's Fees. In the event of any Arbitration, action to compel Arbitration, action to enforce an Arbitration award or action to seek injunctive relief pursuant to this Agreement, the prevailing party in such proceeding shall be entitled to an award of their reasonable attorneys' fees and costs for each such proceeding, including the Arbitration, trial and for all levels of appeal.

E. Injunctive Relief; Cumulative Remedies. Each party agrees that a violation or breach of any of the ownership or non-disclosure provisions of this Agreement could cause irreparable harm to the non-breaching party for which monetary damages may be difficult to ascertain or an in adequate remedy. Therefore, each party will have the right, in addition to its other rights and remedies, to seek and obtain injunctive relief for any violation of the ownership or non-disclosure provisions of this Agreement, and each party hereby expressly waives any objection, in any such equitable action, that the other party may have an adequate remedy at law. The rights and remedies set forth in this Agreement are cumulative and concurrent and may be pursued separately, successively or together.

15. NON-DISCRIMINATION. Contractor does not discriminate against any employee or applicant for employment on the basis of their age, race, religion, color, marital status, sexual orientation, sex, disability, national origin, or ancestry.

16. SUB-CONTRACTING. For the purposes of this Agreement, Contractor shall not utilize third parties or sub-contractors unless Client has agreed to such in writing prior to their starting work. In the event a sub-contractor or third party is used to fulfill any part of the Services within this Agreement, they will be required to provide proof of adequate insurance and be bound by the confidentiality and non-discrimination sections of this Agreement.

[Signature page to follow]

IN WITNESS WHEREOF, the City of XXXX and IT STRATEGIES GROUP, LLC have duly authorized, executed and entered in this Agreement.

XXXX

Signature	
Print Name:	
Title:	
Date:	
Address:	
Email Address:	

IT STRATEGIES GROUP, LLC

Signature	
Print Name:	Kevin McDaniel
Title:	President
Date:	October 19th, 2025
Address:	601 Knightsbridge Road Waunakee, WI 53597
Email Address:	kevin.mcdaniel@it-strategies-group.com

Contract Schedules

Schedule A - Service Offering

Below are the components that make up the support agreement provided by IT Strategies Group. For a more detailed listing of the technologies and services covered within this agreement, please refer to Appendix B.

IT Security:

IT STRATEGIES GROUP, LLC, utilizes a 'defense in depth' methodology in its approach to network security. This includes:

- 24 / 7 monitoring by our Security Operations Center.
- Ongoing vulnerabilities scanning (All event logs, and other gathered telemetry is sent to SOC's AI, which looks for patterns of known breaches and / or anomalies to the client's known use and traffic patterns.
- Ongoing Patch Management of operating system(s) and functions
- Annual penetration testing.
- Monthly scanning of the dark web for compromised staff accounts.
- Endpoints have Endpoint Detection & Response (EDR), which not only feeds the SOC AI telemetry, but also allows the AI to immediately (in time measured in hundredths of a second) isolate a device if it appears to be compromised.
- Endpoint cloud-based backup and recovery services
- Ongoing security vulnerability scanning
- Automated ability to inventory all hardware / software within the environment.
- Ongoing user security training, to ensure staff are trained in identifying cyber threats.

Infrastructure Monitoring /Management:

IT STRATEGIES GROUP, LLC monitors, manages, and maintains the infrastructure including Servers, Storage, LAN, and WAN to ensure maximum uptime and reliability in systems. Included in this offering:

- 24/7 monitoring and alerting on network devices.
- LAN/WAN Support (including interface with telecommunications provider)
- Server & Storage Monitoring and Management
- Security monitoring of MS 365 accounts

- Backup & Restore
- Infrastructure Application Support (Office 365, SharePoint, Citrix, VMWare, etc.)
- Ownership of Support Relationship with IP Telephony Vendor
- Support of All of the Above, Whether on Premises or In Cloud

Endpoint Management:

Managing PCs and mobile devices presents a problem for many organizations today. Organizations look to increase employee productivity, often remotely, while securing all data and thus a constant need for upkeep and support on these devices exists. IT STRATEGIES GROUP, LLC provides easy, secure, and reliable support for all end point devices on the network. Included in this offering:

- PCs (Hardware and Operating System)
- Application Monitoring & Support - VPN, VMWare, Office 365, Active Directory
- User Management & Training
- Proactive Resource Monitoring
- Ability to Apply & Monitor Security Settings to Ensure Compliance with IT Security Program and Policies

Strategic Planning:

Many organizations overlook the IT investments necessary to support a new offering or expand on their existing line of services. IT STRATEGIES GROUP's team of engineers and Architecture Account Managers will work together with The City of CLIENT to ensure that the IT budget is invested wisely and predictably. Included in this offering:

- Fractional CIO/IT Director/Architecture role
- Capacity Planning
- Emerging technologies research
- Business Continuity Design and Testing
- Procurement Assistance
- Periodic Technology Reviews (Frequency to be Set by Client)

Client Responsibilities

Although IT STRATEGIES GROUP, LLC strives to be able to service our client's entire IT needs, certain responsibilities remain with The City of CLIENT's staff. Among those responsibilities is warranty support on all devices under management. Due to the complexity and wide variety of technologies in any environment, it is crucial to keep manufacturer warranties current and with appropriate support levels. Further client responsibilities are as follows:

- Help drive acceptance and adherence to IT Security Programs and support IT security policies and practices, including all auditing, annual risk assessments, etc..
- Firewall license, manufacturer support and/or warranty (ITSG will help report and manage licenses, Client must purchase)
- Router and switch manufacturer warranty (24/7 for core devices and 8x5 (normal business hours) for others) (ITSG will help report and manage licenses, Client must purchase)
- To notify IT STRATEGIES GROUP, LLC of any changes initiated by Client within covered systems.
- Agree to license and run IT STRATEGIES GROUP's standard security and management software.
- Backup hardware and software licensing, manufacturer support and/or warranty (ITSG will help report and manage licenses, Client must purchase)
- Keeping genuine, licensed, and vendor-supported Server and Desktop Software (ITSG will help report and manage licenses, Client must purchase)
- Committing to secure and encrypted wireless data traffic in all offices.
- Maintenance and updates of Business Continuity Plan (ITSG will help create program, Client must be committed to reporting all changes that impact the business continuity plan
- Annual testing of systems recovery
- Line of Business application support (ITSG will take ownership and work with 3rd party vendors to resolve issues, Client provides all application use support to their staff)
- Client agrees that IT Strategies Group personnel will be part of all meetings that involve technology

Change Requests

A **Change** is defined as an Add/Change/Remove to an existing component/environment. All change requests require client approval whether covered by the monthly contract or not. There are two types of Change Requests, **Standard** and **Non-Standard**. **Standard Changes** (those that occur regularly in maintaining an IT environment) are included services within this agreement. **Non-Standard Changes** introduce new functionalities, capabilities or technologies into the environment. These are not included and are explained further in "***Schedule B: Excluded Services***" section of this document.

Standard Change Requests

All **Standard Change Requests** (any change requests needing less than 30 minutes of continuous engineering time) are included in this contract. Examples of **Standard Change Requests** are as follows:

- Non-major version upgrades to devices under management (Patches)
- Service pack installations
- Adding switch ports to a VLAN
- Adding / removing users
- Rebuilding of workstations

Appendix A - Service Levels Targets and Escalation Details

The following table shows the target of response and resolution times for each priority level.

Trouble	Priority	Response Time	Escalation Threshold
Service is not available (all users and functions are unavailable)	Critical	Within 30 minutes	1.5 hours
Significant degradation of service (large number of users or business critical functions affected)	High	Within 1 hour	3 hours
Limited degradation of service (limited number of users affected, business process can continue)	Medium	Within 4 hours	6 hours
Small service degradation (business process can continue, 1 user affected)	Low	Within 12 hours	18 hours
Asking for a quote, review of possible new technology or provide IT information	Info	Within 72 hours	144 hours

Support Tier	Description
Help Desk (Tiers 1 & 2 Support)	All support incidents begin at the Help Desk, where the initial trouble ticket is created, the issue is identified and clearly documented, and basic hardware / software troubleshooting is initiated. Target is for 80% of all tickets to be resolved here.
Tier 3 Support	All support incidents that cannot be resolved at the Help Desk are escalated to Tier 2, where more complex support on hardware / software issues can be provided by more experienced engineers.
Tier 4 Support	Support incidents that cannot be resolved by Tier 3 Support are escalated to Tier 4, where support is provided by the most qualified and experienced engineers who have access to collaborate with 3rd Party (Vendor) support engineers to resolve the most complex issues.

Appendix B - Service Offering Details

Network Security

Description	Frequency
Check Firewall logs for errors	Realtime
Check SPAM Firewall logs for errors	Realtime
Check Web Filter logs for errors	Realtime
Apply necessary Firewall software and firmware updates	Weekly (as needed if priority by vendor)
Apply necessary SPAM Firewall software and firmware updates	Monthly
Apply necessary Web Filter software and firmware updates	Monthly
Apply SPAM Firewall definition updates	As Needed
Apply Web Filter definition updates	As Needed
Adjust Firewall rules	As Needed
User / Access administration and white-listing for SPAM firewall	As Needed
User / Access administration for Web Filter rules	As Needed
Annual Security Audit	Annually
Act as liaison w/ SOC	As Needed
Wireless Access Point Management	As Needed

Infrastructure Management

Description	Frequency
Manage & maintain infrastructure applications listed below: • MS Active Directory • MS SQL (regular maintenance) • MS SharePoint (regular maintenance) • MS Storage Server • Networked Attached Storage	As Needed
VMware (V3 and Vsphere) Citrix Presentation / XenApp Server	As Needed
Monitor MS Applications Event Log to identify potential issues	Upon Request
Monitor MS System Event Logs to identify potential issues	Realtime (servers) – As Needed (Endpoints)
Identify potential hardware / device issues	Realtime
Confirm date and success of last virus scan performed	Realtime
Review disk space status for all drives to identify potential issues	Realtime
Monitor disk space usage	Realtime
Monitor CPU percentage utilization to identify potential issues	Realtime
Run defrag on all drives	Quarterly

Description	Frequency
Perform disk cleanup activities (if applicable / approved by client)	Upon Request
Perform scheduled service during approved service window	Weekly
Reboot servers	As Needed
Perform Activity Directory Administrative Tasks: • Add / Change / Delete / Unlock Users • Add / Change / Delete Groups • Assignment of individual users and group access rights • Minor group policy and site & services administration	As Needed
Review of backup logs to identify potential issues	Realtime
Perform test restore from backup	Annually, Quarterly if Client has Resources
Review Exchange information store size	Not Needed City's Exchange in Azure
Review messaging-specific application errors to identify potential problems	As Needed

Description	Frequency
Alert client to dangerous conditions: • Virus infection / outbreak • Potential data corruption • Potential hard drive failure • Hard drive running out of disk space • Low available memory • Network connectivity errors • System or Application events that may result in service distribution • General backup failure • Media failure • Media rotation failure • Significant inconsistency of backups due to any issue	Realtime
Continually enhance monitoring to track network performance proactively	Ongoing
Install hardware (server, network, storage)	As part of a non-standard change
Configure hardware (server, network, storage)	As Needed
Apply patches and firmware updates	Weekly (unless priority by vendor)
Troubleshoot and resolve circuit and non-circuit network outages	As Needed
Handle routine network administration and maintenance	As Needed
Implement centralized authentication to allow password changes and users specific logons	As Needed

Description	Frequency
Keep IT system's documented and accessible	Ongoing
Continually review the network with regards to security vulnerabilities or abnormal traffic	Realtime
Act as liaison with the City of CLIENT and NOC / SOC	As Needed

Cloud Management

Description	Frequency
Manage & maintain following cloud components: • Entre Active Directory • Microsoft (Office) 365 • SharePoint (regular maintenance) • Entre Virtual Machines • Entre Databases (CSMOS and SQL) • Storage Accounts • Entre Networking	Ongoing monitoring and management are part of ongoing services. Implementation of cloud services are considered non-standard changes and will be billed out as chargeable projects.

End Point Management

Description	Frequency
End user workstation setup and training	As Needed (new endpoints are treated as non-standard changes, and have a nominal fee for setup)
Report on the disk space status for all drives	Realtime
Run defrag and check disks on all drives (if applicable / approved by client)	As Needed
Perform disk cleanup activities (if applicable / approved by client)	Upon Request
Run system restore point backups	As Needed
Recover files / folders / endpoint when needed	As Needed
Identify and deploy management agent to new devices found on LAN scan	Realtime
Unlimited help desk calls through service desk	For infrastructure and security support, does not include application support
IT STRATEGIES GROUP will attempt to resolve all incidents remotely	As Needed
Ticket reporting	Quarterly
Alert client to conditions impacting performance: • User in need of training • Trending of unhealthy PCs	Quarterly
Triage calls by priority and user	As Needed
IT STRATEGIES GROUP Service Desk supported tasks: • PC Software support	Realtime

Description	Frequency
○ PC Desktop settings (i.e. email, network, printer, monitor) ○ PC Desktop Hardware support (phone number for hardware support needs, support with peripheral devices, etc.) ○ User Administration- Add / Change / Delete / Unlock or password reset ○ VPN or Citrix Client • PC Desktop Settings (i.e., email, network, printer, monitor) • PC Desktop Hardware Support (phone number for hardware support needs, support with peripheral devices, etc.) • User Administration- Add / Change / Delete / Unlock or password reset	
Work with and act as liaison with hardware manufacturer to apply equipment warranties and repairs	As Needed

Strategic Planning

Description	Frequency
Participation in IT Steering Committee Meetings	Quarterly
Executive Strategy Meetings	Quarterly
Emerging Technology Research	Ongoing
Presentation for improvements or emerging technology update	As Needed
Executive Reporting	Monthly
Business Continuity Plan Testing	Semi-Annually
IT Budget Development	Annually
IT Governance Review and Development	Ongoing
IT STRATEGIES GROUP IT Security seminars for all clients	Quarterly
Procurement	As Needed
Participation in Regulatory / Compliance meetings	As Needed

Schedule B - Excluded Services

Non-Standard Changes:

Non-Standard Changes are defined as series of tasks that introduce new functionalities / capabilities / technologies and have a defined start and end date.

Examples include:

- Major software version upgrade (Windows 2007 to Windows 10;Exchange 2007 to 2010, OnBase version 18 to version 22, etc.)
- Migrating from the Microsoft business tenant to the government tenant.
- Migration to the cloud
- New Datacenter Implementation
- New Branch Office/Location
- New VLAN Implementation
- Adding a new security program
- Server upgrades and installs
- Endpoint installs (if exceeding 5 per month, or if excessively complex)
- IT Wiring
- Support tickets that have exceeded 2.5 hours of IT Strategies Group effort and appear to require more than 2.5 hours more to resolve.

Emergency Support:

The CLIENT may need support for end users on an emergency basis and outside the normal business hours covered by IT STRATEGIES GROUP's Service Desk*. This after-hours emergency support will be redirected to the appropriate resources and will be handled on an as needed basis. An IT STRATEGIES GROUP engineer responds to the emergency system 24 hours a day, 7 days a week.

**The standard IT STRATEGIES GROUP, LLC "NOC" hours of operation for providing the Services are between the hours of Seven (7) a.m. and Seven (7) p.m. Monday through Friday, excluding holidays ("Standard Service Desk Hours"). For work needing to be done outside those hours, unless previously agreed to by both parties, the standard hourly rate for Systems Support Engineer ($150 / hour) will be charged.*

IT Rates for Non-Included Work (Major Changes & Projects) & Discount Rate

Expertise	Standard Rate	Discounted Rate
Architect	$252	$226
System Support Engineer	$134	$110
NOC Engineer	$140	$120
SOC Engineer	$252	$226

Schedule C – Fees

Device Type	# Devices	Standard Cost / Device / Month	Standard Extended Cost / Month	Municipality Discount / Device / Month	Total Net Monthly Cost
Workstations		$139		$47.68	
Servers		$139		$47.68	
Routers		$77		$10.00	
Storage (NAS)		$77		$10.00	
Printers		$65		$5.00	
Sites		$100		$200	
Phones		$25		$0	
		Total		**Total**	

NOTES:

1. SOC EDR is provided through our deployment of security tools on both endpoints and servers.
2. SOC 24/7 Network Monitors, covers monitoring of logs and network traffic for servers and firewalls for threats and notification if threats are found.
3. Fees are for the number of devices and locations listed in the preceding table. Details listed in Appendix B. Each month IT Strategies Group will true-up the number of devices for billing, in AutoTask, RMM and Microsoft licensing.

- - -Signature Page Below- - -

IN WITNESS WHEREOF, the CLIENT and IT STRATEGIES GROUP, LLC have duly authorized, executed and entered in this Agreement.

CITY OF CLIENT

Signature	
Print Name:	
Title:	
Date:	
Address:	
Email Address:	

IT STRATEGIES GROUP, LLC

Signature	
Print Name:	Kevin McDaniel
Title:	President
Date:	August 4th, 2025
Address:	601 Knightsbridge Road Waunakee, WI 53597
Email Address:	kevin.mcdaniel@it-strategies-group.com

References

Jared Heyn
Deputy Village Administrator
Village of Waunakee
(608) 849-3015

Renee Meinholz
Finance Director
Village of Waunakee
(608) 850-6622

Guy Starbuck
Chief Technology Officer / Co-Founder
AIQ Solutions
(608) 512-7391

Other References Provided Upon Request

Response to Police Department Records Mgt & CJIS Migration

IT Strategies Group assumes that the City of Eagle River will benefit from creating and launching a full-city IT security program — including policies, clear processes and documentation. We'll adapt our proven security policy templates and manage the initial implementation, estimated at about 15 hours. Because the City also interacts with law-enforcement data, we'll support adapting those policies to meet the baseline standards required by Criminal Justice Information Services Division (CJIS) — with an additional estimated 10–15 hours of effort, depending on how much support is needed to set up your document-management system for compliance.

Location & Service

At **IT Strategies Group**, we serve clients around the world—from Australia and Germany to Norway and the United States—bringing wide-ranging experience to every engagement. Our help desk resolves over 90 % of calls at first contact via phone or remote session, while our system administrators successfully handle nearly 100 % of support tickets and project tasks remotely. For the City of Eagle River, we plan for one of our senior technicians to be onsite for approximately 3-5 days during the onboarding phase. Thereafter, your Technical Account & Advisory Manager (TAAM) or senior technologist will visit your site once per quarter, or more frequently based on project needs. All hardware orders are managed from our Waunakee office, pre-configured and shipped directly to your location—ready to go. If the City desires more frequent onsite visits, we are open to exploring options to meet that requirement.

High-Level IT Security Assessment & Current State Architecture For

CITY OF EAGLE RIVER Wisconsin

Prepared By:

IT Strategies Group, LLC

Date:

October 19th, 2025

601 Knightsbridge Road
Waunakee, WI 53597
it-strategies-group.com

Terminology | IT Security

Term or Acronym	Definitions
Anti-Virus	Program that protects your computer or devices from harmful software, like viruses, spyware, or ransomware. It scans your files and system for anything suspicious, blocks or removes threats, and helps keep your data safe.
Malware	It is any kind of bad software that's made to harm your computer, steal your information, or cause problems. This includes things like viruses, spyware, ransomware, and worms. It is one of the type of things that Anti-Virus software looks for.
Phishing	A scam where someone pretends to be a trusted source (like a bank or coworker) to trick you into giving away personal information — such as passwords, credit card numbers, or login details.
SPAM	Unwanted or junk messages — usually emails — sent in bulk, often for advertising, scams, or spreading malware.
Ransomware	Is malicious software that locks or encrypts your files and demands payment (a ransom) to unlock them.
Backup & Recovery	Is the process of **saving copies of your data** (backup) and **restoring it** (recovery) if it's lost, deleted, or damaged — helping you get your information back after a problem like a crash, attack, or hardware failure.
IT Security Policies	Aare a set of **rules and guidelines** that explain how a company protects its computer systems, data, and networks — and what employees must do to keep information safe from threats or misuse.
CJIS	**Criminal Justice Information Services**. It's a division of the FBI that manages and protects sensitive law enforcement data — like criminal records and fingerprints.
IT Security Program	An **IT Security Program** is the **overall framework** a company uses to **protect its information and technology assets**. It's the *big picture* — the strategy, structure, and ongoing processes that ensure information security is managed effectively across the organization.
IT Steering Committee	An **IT Steering Committee** is a **governance body** that provides **strategic direction, oversight, and accountability** for an organization's information technology and information security management efforts.
Risk Assessments	A **Risk Assessment** is the **systematic process** of identifying, analyzing, and evaluating risks that could negatively impact an organization's information assets.

Annual IT Security Review	An **Annual IT Security Review** is a **formal, periodic evaluation** of an organization's information security management prgram (ISMS), technology controls, and overall cybersecurity posture to ensure ongoing compliance with **ISO 27001 requirements** and continuous improvement.
Annual Strength, Weakness, Opportunities & Threats (S.W.O.T.) Analysis	A **S.W.O.T. Analysis** — which stands for **Strengths, Weaknesses, Opportunities, and Threats** — is a **strategic assessment tool** used to understand the **internal and external factors** that can impact an organization's **Information Security Management Program (ISMP)**.
Business Continuity	**Business Continuity** is an organization's ability to keep essential operations running during and after disruptions — like cyberattacks, disasters, or system failures — through prepared plans, processes, and resources that minimize downtime and impact.

Terminology | IT Architecture

Term or Acronym	Definitions
IT Architecture	**Definition:** A clear picture of the technology, systems, and processes an organization uses today. **Why it helps:** It shows what's working, what's outdated, and where problems exist — providing a baseline for improvement.
Current State Architecture	**Definition:** A clear picture of the technology, systems, and processes an organization uses today. **Why it helps:** It shows what's working, what's outdated, and where problems exist — providing a baseline for improvement.
Future State Architecture	**Definition:** A vision of how the organization's technology should look in the future to meet business needs. **Why it helps:** It guides planning and investment so technology evolves in step with the company's goals.
Gap Analysis	**Definition:** The process of comparing the current state to the future state to find what's missing or needs improvement. **Why it helps:** It identifies specific changes — like new systems or upgrades — needed to reach the desired future state.
Roadmap	**Definition:** A step-by-step plan showing how and when to move from today's technology setup to the future vision. **Why it helps:** It provides a clear timeline and priorities, helping leadership coordinate projects, budgets, and resources effectively.

Contents

Terminology | IT Security ..... A
Terminology | IT Architecture ..... B
Document's Scope: 1
Overview 3
Purpose 3
Findings Summary 3
Next Steps 4
Methodology: 4
Current State Architecture 5
Driving Needs / Requirements 5
Hardware Inventory 5
Software Inventory 6
Security Inventory of Services 6
Anti-Virus (AV) 6
Endpoint Detection & Response (EDR) 6
PHISING & SPAM Filter 7
DarkWeb Scanning 7
Endpoint Backup 7
SaaS Backup (Microsoft Office Online) 7
Services & Administrative Account Password Rotation 7
User Password Vault 8
Multi-Factor Authentication 8
Ongoing User Security Training 8
Continuous Vulnerability Scanning 8
7 x 24 Security Operations Center 9
Annual External Network Penetration Testing 9

IT Security Program & Policies 9
Compliance Management 9
IT Support Services (In addition to the security services listed above) 10
IT Ticketing System 10
Remote Monitoring & Management System 10
IT Inventory & Process Documentation 10
Dedicated Helpdesk 10
Dedicated System Engineers 11
Project Management Systems & Management 11
IT Operations Assessment Summary 12
IT Security & Recoverability Assessment 14

Executive Summary:

High-Level IT Security Assessment & Current State Architecture for the City of Eagle River
Prepared by IT Strategies Group, LLC – October 19, 2025

Why this matters

Your municipality's technology systems support every department and service—from public safety and record-keeping to everyday administrative work. Yet, many of these systems are showing signs of strain. Ensuring your IT environment is secure, reliable and aligned with your goals is more important than ever, particularly as cyber threats increase and grant funding windows are limited.

Key Findings & Drivers

- **Limited IT support capacity**: Your current IT services provider is a single individual. If that person is unavailable (due to illness or vacation), coverage lapses. In addition, the provider appears unable to keep pace with the City's current IT and security demands.
- **Remote access issues**: VPN connections are unreliable—users experience frequent failures to connect, or get disconnected mid-session, which inhibits remote work and operational flexibility.
- **Public safety systems shifting**: The Police Department is being required by the current provider (Vilas County) to switch providers—this includes handling systems with sensitive access (CJIS). The plan is to move these services in-house, creating urgency for stability and compliance.
- **Grant deadlines driving urgency**: The City wants to tap State cyber-grant funds and innovation-grant funds to upgrade IT systems and security. These grants impose tight deadlines, making it critical to act quickly.
- **Infrastructure upgrade needed**: An internet-connectivity upgrade with Norvado is planned, indicating that current connectivity may not fully support future demands.
- **Security and process gaps**: Across the board, we found uneven deployment of security tools and inconsistent processes—creating risk and inefficiencies.

Recommended Next Steps

1. **Select a new managed-services partner** (target January 1, 2026) to increase support capacity, reduce single-point dependence, and raise IT and security standards.
2. **Prioritize urgent remediation (next 90 days)**:
    - Stabilize remote access/VPN connectivity.
    - Ensure critical public-safety systems (CJIS access) are managed securely and transition plans are clear.
    - Deploy basic security controls city-wide (endpoint protection, MFA, backups).
3. **Build a 12-month strategic roadmap** aligned with upcoming grants and your operational goals to modernize infrastructure, streamline systems, enhance cybersecurity, and make operations more efficient.
4. **Begin immediate risk mitigation steps**:
    - Finalize the Norvado internet upgrade.
    - Strengthen documentation and processes so grant applications and compliance tasks are supported.
    - Move key systems and departments from reactive support to proactive management.

What you need to decide now

Decision	Purpose
Contract a managed-services partner	To provide reliable, scalable IT support, reducing risk from relying on one person.
Allocate budget for first-phase upgrades	To stabilize essential systems (VPN, internet) and meet imminent grant deadlines.
Sponsor a technology steering committee	To oversee strategy, prioritize investments, and align IT with the City's mission and services.

Impact

By taking these actions now, the City will reduce the risk of a disruptive cyber-incident, improve reliability of essential services, gain access to grant funding, and position itself to operate more efficiently—ultimately delivering better service at a lower long-term cost for taxpayers.

Document's Scope:

Overview

As part of IT Strategies Group's initial discovery process, a **high-level IT Security and Current State Architecture Review** was conducted for the **City of Eagle River**.

The goal of this assessment was to gain a clear understanding of the City's existing technology environment, evaluate its cybersecurity posture, and identify areas where **managed IT services** could provide measurable operational and strategic value.

Purpose

This review was designed to help city leadership:

- Understand the **current state of IT systems, infrastructure, and security**.
- Identify **gaps, inefficiencies, and risks** affecting reliability, performance, and compliance.
- Reveal **opportunities to improve service delivery** through proactive management and modernization.
- Establish a foundation for **strategic partnership** with IT Strategies Group in supporting long-term technology goals.

Findings Summary

The review identified several opportunities to enhance the City's IT environment, including:

- Improved **network performance and standardization** across departments.
- Strengthened **cybersecurity controls** and monitoring practices.
- Enhanced **data protection and recovery capabilities**.
- Potential **cost efficiencies** through consolidation and proactive managed services.

Next Steps

IT Strategies Group will work with City leadership to:

- Submit, and hopefully win, our response to the City's RFP (attached with this document).
- Perform a complete current state discovery and follow onboarding process documented in our RFP response.
- Prioritize findings and define **short-term remediation goals**.
- Develop a **Managed IT Services plan** tailored to the City's operational, security, and budgetary needs (part of our onboarding process, see RFP response).
- Establish a **strategic technology roadmap** to support scalability, compliance, and future growth.

Methodology:

The methodology used is a scaled own version of the methodology we use to onboard our new clients.

- Interview of key stakeholders at the City of Eagle River to determine:
  - What they like in their current IT structure.
  - What they feel are challenges.
  - What they are reacting to (outward pressures).
  - Where they would like to see their environment over the next year, two years and three years.
  - Establish baseline known inventories (Network, Servers, Endpoints (workstations & laptops) and Applications).
- Utilize Discovery Tools
  - Send prospective client end-user initiated scanning application that will scan each device for known vulnerabilities and then try to scan network from each of scanned endpoints. Utilize the output to determine high-level security issues analysis
  - Send prospective client cyber hacking assessment tool. If anti-virus is not present or not correctly configured, this application scans for ports and whether it can write to or read from restricted resources
- Create report (this document) on findings

Current State Architecture

Drivers for Eagle River's IT Managed Services Change

- Current IT services provider is a one (1) person operation.
  - Coverage when this person is sick or on vacation (this has occurred)
  - Current managed service provider doesn't seem prepared to keep pace with the City's IT needs and IT security in general
- There have been issues with support of VPN, which cannot connect often, when they do connect, it often disconnects
- The Police department is being required by their current provider (Vilas County) of police department systems (including CJIS access) to switch providers (current plan is to move it in-house).
- Desire to utilize State cyber grant funds for portions of upgrading IT systems / IT security (this forces a short time frame to meet grant submission deadlines)
- Desire to utilize State innovation grant funds form some of the IT services expenses (again, forcing a shorter time frame to meet grant submission deadlines)
- Internet connectivity upgrade with Norvado
- Plan is to transition to new IT managed services provider (we would love it to be us) on January 1st, 2026

Hardware Inventory

The end-user-initiated discovery tool was run on the following endpoints:

- 2025-DPW-DESKTP
- CLERK-LAPTOP
- DESKTOP-314M7KV
- LAPTOP-UBGHF46B

Discovered during interview:

- Total of 18 endpoints, spread between 4 locations
- 1 server located at the Administration Building
- 1 network (router & switches) at each of the locations, each connected to the internet
- 40 phone lines

Software Inventory

- Microsoft licenses:
  - Six (6) E3 licenses
  - 9 emails (including shared resource emails)
  - 8 to 9 additional email addresses that will need to be migrated to the City's environment, as part of the police department transition
- Key City Software Systems:
  - Work & Hours (Civic Systems)
  - Golf Now
  - Website (Blue Host)
  - Dog Licensing (?)
  - ArcGIS (Contracted to engineering firm)

Security Inventory of Services

Anti-Virus (AV)

Anti-virus software scans systems to determine if known software patterns exist on the machine indicating that a cyber criminal has successfully (through many different means) has placed ransomware, malware or other software that performs malicious actions in a way that compromises data on that system.

The City of Eagle River has some systems that are running Sophos Intercept X and some are running only Windows Defender (rudimentary AV solution). It is important that a standardized and centralized AV solution be in place, that prevents users from turning it off or changing its configuration. The City of Eagle River's solution does not meet these standards.

Endpoint Detection & Response (EDR)

An EDR system monitors each computer and laptop for unusual activity — if one starts acting differently, it may have been compromised.

The City of Eagle River has a non-managed implementation on some of its devices of Sophos, which is a consumer grade (not enterprise grade) EDR solution, but it is not centrally managed, not configured with controls that ensure it is monitored in a way consistent with the City's security policies. It is also not standardized, because it is not on all devices.

PHISING & SPAM Filter

These filters check incoming email for dangerous links or attachments (phishing) and for mass-mailed junk messages (spam). In either case, the filter blocks the email before you see it — meaning fewer harmful emails to click on and fewer spam messages to sort through.

T*he City of Eagle River does not have any PHISHING & SPAM filtering technology deployed*.

DarkWeb Scanning

This technology scans the dark web (the deep web, where cyber criminals compare notes and sell victim data), for user credentials that are being listed for sale.

The City of Eagle River does not have this technology deployed.

Endpoint Backup

No matter how hard IT tries, users keep saving files to their devices. Unfortunately, server focused backups do not protect that data and endpoints are more likely to fail than servers, so that data is often lost. Endpoint backup backs up a user's workstation / laptop.

The City of Eagle River does not currently have endpoint backup technology deployed.

SaaS Backup (Microsoft Office Online)

Many organizations assume that Microsoft OneDrive and other Microsoft 365 services automatically back up all their files and data. In reality, although Microsoft provides infrastructure resilience, recovering from deleted files, ransomware or a major incident is the organization's responsibility unless a dedicated backup solution is in place.

The City of Eagle River does not currently have this technology deployed.

Services & Administrative Account Password Rotation

Since service accounts (used by applications) and administrative accounts (used by IT staff) have very high access, it's critical to change their passwords regularly—ideally at least every six months—to reduce the risk of unauthorized access.

The City of Eagle River does not have this technology deployed at this time.

User Password Vault

A password vault securely stores your log-ins and only lets you access them after you've confirmed your identity (for example with a fingerprint or a code). Then it can fill in long, strong passwords for you — so you don't have to write them down or reuse weak ones.

The City of Eagle River does not have this technology deployed.

Multi-Factor Authentication

Multi-factor authentication (MFA) asks you to log in with your usual user ID and password **and then** verify your identity with a second method—such as a phone prompt, app code, or key fob—so even if someone steals your password, they still can't access your account. This extra layer boosts security, helps prevent data breaches, and protects your organization's systems.

The City of Eagle River does not have this technology in place.

Ongoing User Security Training

People are often the weakest link in an organization's security. Regular training helps employees spot common threats like phishing emails. A strong program sends out monthly lessons, quizzes, and simulated attacks. It checks who opened the fake email, clicked a link, or entered credentials — so the organization can target extra training where it's needed. Doing this turns familiar users into an effective line of defense.

The City of Eagle River does not currently have this technology.

Continuous Vulnerability Scanning

Constantly scanning systems for known weaknesses helps the organization spot risks from new software or updates before attackers can exploit them, and includes clear guidance and tracking to fix those issues fast.

The City of Eagle River does not have this technology.

7 x 24 Security Operations Center

A Security Operations Center (SOC) is a team of security experts working around the clock to monitor an organization's systems, detect unusual activity, and respond quickly to threats — helping protect data and keep operations running smoothly.

The City of Eagle River does not have this available to them today.

Annual External Network Penetration Testing

Traditionally, annual penetration tests — involving expert hackers probing systems — cost tens of thousands of dollars. With our solution, you can get a more affordable automated test that checks your network from the outside, reveals whether attackers could break in, and gives us clear steps to fix any gaps.

The City of Eagle River does not have this available to them today.

IT Security Program & Policies

An IT security program is a set of policies (rules outlining how your technology should be used) together with the processes that make sure those rules are actually followed across the organization.

The City of Eagle River has some IT security policies but does not have

Compliance Management

Compliance management is the process by which an organization uses tools, policies and controls to ensure it meets all relevant legal, regulatory and certification requirements — and keeps clear evidence that it's done so.

The City of Eagle River does not have this capability today.

IT Support Services (In addition to the security services listed above)

IT Ticketing System

A ticketing system helps track every IT issue or request in one place, making it easier to spot recurring problems, fix the root causes, and show clear documentation for audits or compliance.

The City of Eagle River does not have this available to them today.

Remote Monitoring & Management System

A Remote Monitoring & Management (RMM) system lets your IT team keep an eye on all your computers, servers and devices from one central dashboard, spot and fix issues before they become major problems, install updates automatically, and even access a user's device (with permission) to help them — which means fewer disruptions, stronger security and better documentation of what's been done.

The City of Eagle River's IT provider does not have this capability today.

IT Inventory & Process Documentation

Keeping an up-to-date list of every device, software program and process your organization uses—and knowing how things like password resets or access approval happen—is essential because you can't protect what you don't know you have. With full visibility, you reduce the risk of someone tricking your help desk or slipping in through an unmanaged device, make smarter decisions about technology investments, and stay on top of security and compliance obligations.

The City of Eagle River's managed service provider does not provide or seem to use this system.

Dedicated Helpdesk

A dedicated help desk gives your staff a single, reliable team to call when IT issues arise—whether it's a forgotten password, a broken printer, or an access problem—allowing most problems to be fixed on the first call. That means less disruption to city services, quicker return to work, better control over who's using which systems, and a clear record of how issues were handled, which supports accountability and compliance.

The City of Eagle River does not have access to a helpdesk today.

Dedicated System Engineers

Dedicated system engineers are your go-to experts who understand your organization's technology inside and out—they monitor and maintain your systems full-time, fix issues before they become problems, tailor solutions for your specific needs, and give you peace of mind knowing your IT infrastructure is secure and running smoothly.

The City of Eagle River has access to this as their current provider is a single person provider, however there is no backup if this person is sick or on vacation.

Project Management Systems & Management

While it's important that your IT partner swiftly fixes day-to-day issues, real value comes when they also identify, plan and lead larger improvement projects — things like upgrading systems, boosting security, or streamlining operations. With proper project management, instead of just reacting, your municipality gets organized and efficient: using clearly defined steps, timelines, and budgets to move from where your technology is today to where it should be, reducing downtime, controlling costs, and letting your staff focus on serving the public rather than fighting fires.

The City of Eagle River does not have this as part of their current IT managed services.

Virtual CIO

A **vCIO (virtual Chief Information Officer)** serves as your municipality's go-to technology strategist, guiding your IT decisions in alignment with your community goals. They help map out long-term plans for infrastructure, cybersecurity, budget and vendor relationships — while your IT support team handles the day-to-day operations. With a vCIO on board, you gain expert advice at a predictable cost, avoid costly technology missteps, improve service delivery, and ensure your systems stay secure, up-to-date and aligned with your city's priorities.

The City of Eagle River's IT provider does not have this capability today.

IT Operations Assessment Summary

Should the City of Eagle River choose IT Strategies Group as its managed IT services provider, we'll follow up this high-level review with a detailed operational assessment. We'll break your IT environment into three key areas—Infrastructure, Security and Service Delivery—and then evaluate nine critical components within them, using a color-coded system (green = good, yellow = needs improvement, red = urgent) to clearly show which parts are doing well and which need attention. The diagram below illustrates our first high-level assessment of the City's managed IT services and

Infrastructure

e.

Figure 1 | Managed IT Services

Figure 2 | Infrastructure

While the summary above may appear concerning, most of the issues stem from missing tools and processes — areas we will address during the first month and refine over the first 90 days. Within days, we'll focus on key areas like workstations, remote access, managed wireless, email systems and cabling, moving their status from red to green, while the remaining items shift from red to yellow as they progress.

IT Security & Recoverability Assessment

Just as we reviewed operational readiness above, we use a similar assessment for the City's security — examining nine core areas of your IT environment and using a color-coded grid (green = good, yellow = needs attention, red = urgent) to show how ready your systems are and where we need to focus improvement

s.

Figure 3 | Security

As with the operations assessment, many of the issues stem from missing tools and processes—which we will begin addressing in the first few weeks and work through in the first 90 days. Our goal is to move most components from red (urgent) to green (good) quickly, while those that require investment or longer fixes will shift to yellow (in progress) and then green according to our agreed strategic roadmap.

FRONTIER SALES PROPOSAL

CITY OF EAGLE RIVER

10/20/2025 – revised 11/10/2025
Quote Number: 00204898R

Heather Saari, Sr Account Executive and
Tatum Westphal, Business Account Executive

Heather: (608) 566-5753

Tatum: (608) 893-0876

Email(s): heather.saari@ftr.com & tatum.westphal@ftr.com

Frontier's contribution to...

Business Challenges & Objectives

- Ensure a highly reliable and secure network for your business and users
- Invest in scalable technology that grows with your future needs

Our Solution

- Modern, fiber-centric network designed for performance and reliability
- A comprehensive portfolio to address both current challenges and future opportunities
- Core principles of speed, simplicity, security and productivity tailored to your needs

Your Business Benefits

- More time to spend on key business priorities through simplified network and communications management
- Professional support by highly skilled technicians, resulting in reduced downtime
- Greater ease in operating and scaling your business as it grows

Our Strengths & References

- Largest US pure-play fiber company
- Over 180,000 miles advanced fiber network
- Best in Biz 2023 and 2022 Product of the Year
- BBB Rating A-

FRONTIER

Who we are

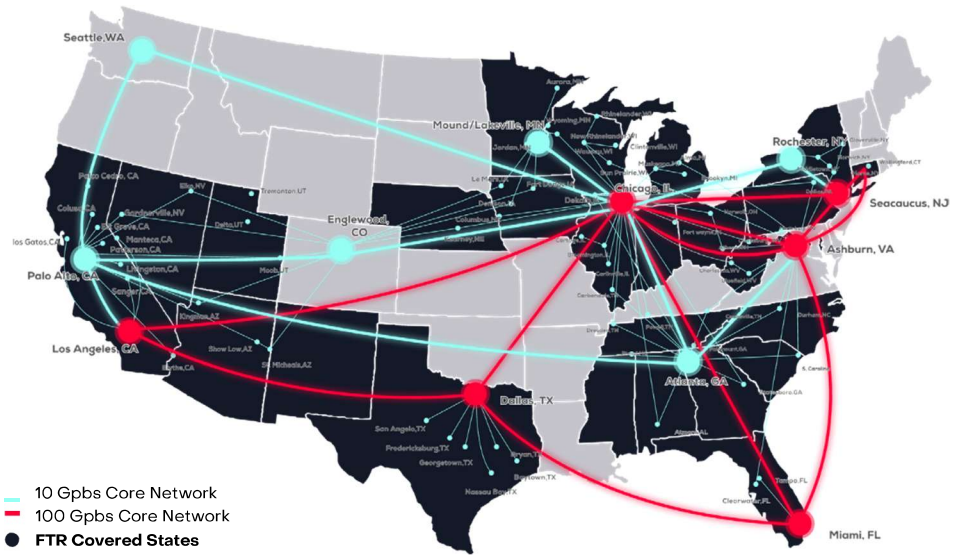
Frontier is leading the “un-cable” revolution. Driven by our purpose, Building Gigabit America™, we are relentless in our pursuit of always delivering a better customer experience. Providing digital infrastructure that empowers people to create the future, we’re connecting millions of consumers and businesses in 25 states with reliable fiber internet and multi-gigabit speeds.

“Frontier is Building Gigabit America . We are deploying fiber and connecting people to the digital society at a record pace . Our team’s operational discipline over the last year has improved Frontier’s financial trajectory and positioned us as the preferred digital partner for customers across our footprint .”

– Nick Jeffery, President and Chief Executive Officer

Our focus, your success

- At Frontier, we believe in the power of technology to change lives. That’s why we take pride in being a trusted business telecommunications partner, helping you meet today’s challenges and technology demands. With more than 180,000 miles of fiber spanning 25 states, our growing network is designed with the evolving needs of business customers like you in mind.
- We know providing better solutions, better service, and better value is the best way to ensure your business wins. From dedicated connectivity to fully managed services, we’re committed to practical and powerful solutions that bring teams together and move businesses forward.



Reliable connectivity, on your terms

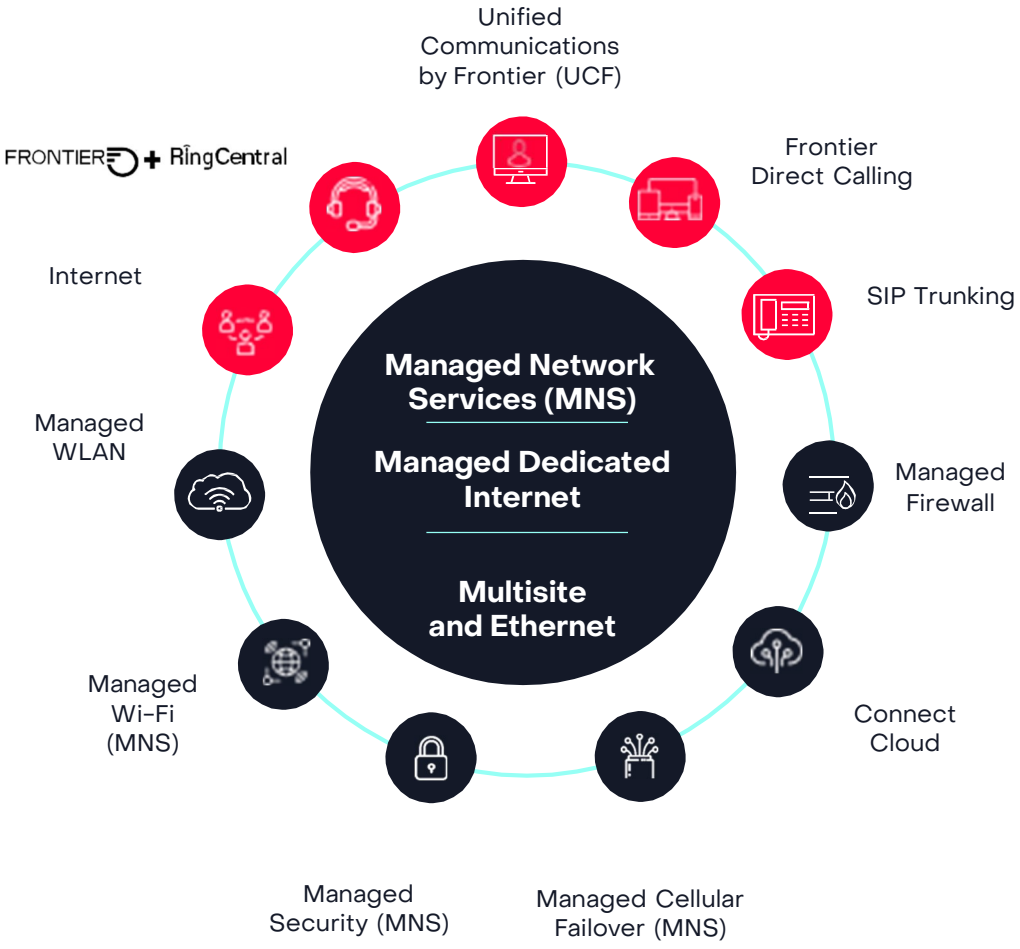
Self-service when you want to, managed & personalized when you don’t.

An Advanced Business Solutions Portfolio

Built with your needs in mind

- **Robust** solutions portfolio for businesses of any size
- **State of the art offerings** with multiple hosting and service options
- **Fully managed solutions** so you can concentrate on your business's critical goals
- **Customizable –** True end-to-end solutions

Strategize | **Deploy** | **Design** | **Manage** | **Integrate** | **Secure**



Executive Summary

We're dedicated to understanding your business challenges. As a result, we can customize a solution that meets your needs and gives you the confidence to move forward.

Our recommendations based on your needs include Business Fiber Internet and Unified Communications by Frontier [UCF].

Business Fiber Internet [Symmetrical download & upload speeds] – 36 Months:

1Gb: $69.99 MRC each*
2Gb: $94.99 MRC each*
5Gb: $119.99 MRC each*
Wi-Fi Extender: $5.00 MRC each (each extender covers 2,500 additional square feet)
*If static IPs are required, additional monthly charges will apply ($20.00 for 1 Static IP or $30.00 for 5 Static IPs).

Unified Communications by Frontier [UCF - VoIP]
Includes one Automated Attendant per entity:

Service Term: 36 Months
Light & Water Shop [2 Phones (1 is Cordless)]
Service Location: 511 Mill St, Eagle River, WI 54521
Total Service Location MRC: $39.75
Total Service Location NRC: $55.00

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	2	36 Months	$0.00	$12.50 x 2 = $25.00
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink T54W [Rental]	1	36 Months	$0.00	$7.50

UCF Yealink W76P [Rental]	1	36 Months	$0.00	$5.25

Service Term: 36 Months
Dept Public Works Shop [4 Phones (3 are Cordless)]
Service Location: 1020 N Bluebird Rd, Eagle River, WI 54521
Total Service Location MRC: $70.25
Total Service Location NRC: $110.00

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	4	36 Months	$0.00	$12.50 x 4 = $50.00
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink T54W [Rental]	1	36 Months	$0.00	$7.50
UCF Yealink W76P [Rental]	1	36 Months	$0.00	$5.25
UCF Yealink W56H DECT HS [Rental]	2	36 Months	$0.00	$2.75 x 2 = $5.50

Service Term: 36 Months
Light & Water Wastewater Treatment Plant [1 Phone]
Service Location: 323 W Division St, Eagle River, WI 54521
Total Service Location MRC: $22.00
Total Service Location NRC: $27.50

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	1	36 Months	$0.00	$12.50
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink T54W [Rental]	1	36 Months	$0.00	$7.50

Service Term: 36 Months
City Hall [5 Phones]
Service Location: 525 E Maple St, Eagle River, WI 54521
Total Service Location MRC: $109.49
Total Service Location NRC: $137.50

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	4	36 Months	$0.00	$12.50 x 4 = $50.00
UCF Executive License	1	36 Months	$0.00	$19.99
UCF Additional DID	1	36 Months	$0.00	$2.00

UCF Directory Listing	1	36 Months	$0.00	$0.00
UCF Yealink T54W [Rental]	5	36 Months	$0.00	$7.50 x 5 = $37.50

Service Term: 36 Months
Police Dept [10 Phones + Call Recording]
Service Location: 525 E Maple St, Eagle River, WI 545218328
Total Service Location MRC: $384.40
Total Service Location NRC: $275.00

Product Name	Quantity	Term Length	NRC	MRC
UCF Executive License	10	36 Months	$0.00	$19.99 x 10 = $199.90
UCF Call Recording Basic	10	36 Months	$0.00	$8.75 x 10 = $87.50
UCF Storage 1 Year	10	36 Months	$0.00	$1.50 x 10 = $15.00
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Additional Directory Listing	1	36 Months	$0.00	$5.00

UCF E911 Additional Site Listing	1	36 Months	$0.00	$0.00
UCF Yealink T54W [Rental]	10	36 Months	$0.00	$7.50 x 10 = $75.00

Service Term: 36 Months
Light & Water [4 Phones]
Service Location: 525 E Maple St, Eagle River, WI 545218328
Total Service Location MRC: $87.00
Total Service Location NRC: $110.00

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	4	36 Months	$0.00	$12.50 x 4 = $50.00
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Additional Directory Listing	1	36 Months	$0.00	$5.00
UCF E911 Additional Site Listing	1	36 Months	$0.00	$0.00
UCF Yealink T54W [Rental]	4	36 Months	$0.00	$7.50 x 4 = $30.00

Service Term: 36 Months
Revitalization [1 Phone]
Service Location: 525 E Maple St, Eagle River, WI 545218328
Total Service Location MRC: $27.00
Total Service Location NRC: $27.50

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	1	36 Months	$0.00	$12.50
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Additional Directory Listing	1	36 Months	$0.00	$5.00
UCF E911 Additional Site Listing	1	36 Months	$0.00	$0.00
UCF Yealink T54W [Rental]	1	36 Months	$0.00	$7.50

Service Term: 36 Months
Golf Course Maintenance Shop [2 Phones (1 is Cordless)]
Service Location: 925 Pleasure Island Rd, Eagle River, WI 54521
Total Service Location MRC: $39.75
Total Service Location NRC: $55.00

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	2	36 Months	$0.00	$12.50 X 2 = $25.00
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink T54W [Rental]	1	36 Months	$0.00	$7.50
UCF Yealink W76P [Rental]	1	36 Months	$0.00	$5.25

Service Term: 36 Months
Golf Course Clubhouse [5 Phones (2 are Cordless)]
Service Location: 457 E McKinley, Eagle River, WI 545218422
Total Service Location MRC: $95.00
Total Service Location NRC: $137.50

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	5	36 Months	$0.00	$12.50 x 5 = $62.50
UCF Yealink T54W [Rental]	3	36 Months	$0.00	$7.50 x 3 = $22.50

UCF Yealink W76P [Rental]	1	36 Months	$0.00	$5.25
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink W56H DECT HS [Rental]	1	36 Months	$0.00	$2.75

Service Term: 36 Months
Eagle River Airport [3 Phones (All are Cordless)]
Service Location: 1311 Airport Rd, Eagle River, WI 545218325
Total Service Location MRC: $50.25
Total Service Location NRC: $82.50

Product Name	Quantity	Term Length	NRC	MRC
UCF Basic License	3	36 Months	$0.00	$12.50 x 3 = $37.50
UCF Additional DID	1	36 Months	$0.00	$2.00
UCF Yealink W76P [Rental]	1	36 Months	$0.00	$5.25
UCF Yealink W56H DECT HS [Rental]	2	36 Months	$0.00	$2.75 x 2 = $5.50
UCF Grand Total			$1,017.50	$924.89

MRC = Monthly Recurring Charges
NRC = Non-Recurring Charges or Installation = $27.50 per phone
DID = Direct Inward Dial

If you decide to purchase the phones instead, here is the pricing, which includes a 1-year manufacturer warranty:

T54W Yealink Phone [Purchase]: $259.00
T54W Power Cord – if needed [Purchase]: $15.00
W76P Cordless Phone + Base [Purchase]: $189.00*
W56H Additional Cordless Handsets [Purchase]: $99.00*
*Power cords included

The services set forth in this proposal will be provided by Frontier Communications and its affiliates (collectively referred to herein as "Frontier").

Frontier does not consider the proposal itself to be a legally binding offer to contract. Pricing contained within this document is budgetary, and a site survey may be required prior to a final quote. This quote is valid for up to thirty days from the date hereof. Taxes and surcharges are not included.