Managed IT Services
Statement of Work

Prepared for

City Of Prairie City

Emily Voeller & Jodie Wyman

Prairie City

Proud of the Past, Confident of the Future.

Prepared by

RK Dixon a Xerox Company

Lance Christenson

Garrin Hathaway

5/24/2022

SUMMARY

City of Prairie City ("Customer") has requested that RK Dixon ("Company") perform defined tasks to provide services on an on-going basis for the specified period, 36 months. This Statement of Work ("SOW") outlines those specific Managed Services to be provided.

This Managed Services SOW is effective as of 5-25-2022 ("Effective Date") by and between Customer and Company pursuant to that certain IT Master Services Agreement ("Agreement") by and between the parties dated 5-25-2025. Capitalized terms used in this SOW that are not otherwise defined below shall have the meanings in the Agreement or schedules, appendices or exhibits to the Agreement.

The following services will be provided to address Customer required needs.

PRICING

Solution Coverage (Subscription Services)	Monthly Services
Managed Helpdesk	**$615.00**
24x7 - Helpdesk Support	
(17) Managed Workstation	
Managed Infrastructure	**$353.00**
24x7 - Device Support	
(2) Virtual Machine	
(1) Physical Server with OS	
(1) Switch	
(2) Firewall/Router	
Fortinet, Cisco	
(2) Wireless Access Point	
Managed Data Protection	**$545.00**
Local/Cloud Backup	
(1) Front-End Data: Up to 2TB	
Monthly Services	**$1513.00**
Monthly Total	
Monthly Total	**$1513.00**

Onboarding, Startup, and One-Time Charges	Price
One-Time Managed Services Onboarding	$ Free
Total Onboarding, Startup, and One-Time Charges:	**$ Free**

Billing will be monthly for the specified SOW duration, 36 months.

ADDITIONAL NOTES:

- Statements of Work are valid for 30 days from the Effective Date.
- Any work performed outside of the scope of this SOW will be billed separately at current rates via a change request.
- Any work performed outside the scope of this SOW will be billed in accordance with the IT Master Services Agreement between the parties and Company's current rates, which include overtime multipliers for work performed outside of 8:00am-5:00pm local time.
- This SOW does not include any formal classroom-based training. Any time spent training Customer will be billed separately at current rates.

PROPRIETARY NOTICE

This proposal contains confidential information of Company. In consideration of the receipt of this document, Customer agrees not to reproduce or make this information available in any manner to persons outside the group directly responsible for evaluation of its contents.

SOW OUTCOMES, DELIVERABLES, AND SCOPE

The goal of this project is to provide Customer ongoing support for the following IT tasks, if included in Solution Coverage:

- Managed Server
  - Includes Virtual Machine, Hypervisor Physical Host, Physical Server with OS, NAS Device, Shared Hypervisor Storage
- Managed Workstation
- Managed Data Protection
- Managed Network Device
  - Includes Switch, Firewall/Router, Wireless Access Point
- Managed Other Device

  Addons:
  - Email Security/Spam Filtering
  - Enhanced Monitoring, Notification, and Reporting
  - Community Portal access
  - Follow Me Filtering
  - Multifactor Authentication

Company will perform the tasks under this SOW while the Customer has a valid agreement and adheres to all the terms in this SOW.

SOW EXECUTION

The tasks below represent the scope of the services to be provided, if included in Solution Coverage:

MANAGED SERVER

WINDOWS SERVER OPERATING SYSTEM SUPPORT

Windows Server Operating System Support includes remote support to return the Operating System to the previous functioning state, patching of the Operating System, and management of built-in server features and roles such as Active Directory Domain Services, DNS, DHCP, File Server, Print Server, and Remote Desktop Services.

Additional software that may be installed on servers such as Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint, Microsoft System Center Configuration Manager are not included as part of Windows Server Operating System Support.

ACTIVE DIRECTORY & GROUP POLICY MANAGEMENT

Company will provide remote support for Microsoft Active Directory Domain Services (AD DS) and Group Policy Management.

AD DS support includes, but is not limited to, adds/changes/deletions of user and service accounts, security groups, and the permissions supporting the organization.

Group Policy Management includes maintenance of existing policies after onboarding and creation of new policies as needed to support the environment.

Testing for AD DS and Group Policy changes may require additional time and/or resources from the customer to ensure expected results are achieved and may incur additional time and materials costs depending on the situation.

ANTIVIRUS

Company offers real-time antivirus threat protection with built in remediation.

EXCHANGE SUPPORT

Company will assist in remote management of Microsoft Exchange Server email environment, including user and license management. Services include adds, changes and deletions of users, distribution lists and mailboxes, password resets, email routing and delivery rule management, assistance with licensing questions, and basic email configuration on supported workstations and mobile devices.

Patching for Microsoft Exchange Server, while not included in this SOW, can be provided as a project on a time and materials basis.

HARDWARE FAULTS

Company will assess hardware faults on covered devices and facilitate repair or replacement by the hardware vendor. The Customer will maintain hardware warranties or provide timely payment for repair charges for any Customer provided equipment covered under this SOW and pay for any costs associated with required upgrades or maintenance agreements to address any new features or security concerns.

ESSENTIAL MONITORING

Company will monitor all supported devices using a standardized monitoring and alerting process for critical services as needed. Automated recovery options are used where appropriate, remote otherwise remediation will be completed by Company.

WARRANTY MANAGEMENT

Company will assist customer in tracking hardware and software contract expiration dates to allow for timely renewal of support or replacement of the covered product.

WINDOWS SERVER PATCHING

Company approves routine patches provided by Microsoft, that are applied to Servers and/or Workstations on a weekly cadence to minimize vulnerabilities and risk.

Company suggested patching schedules and policies are available upon request.

STORAGE DEVICES

Company will provide remote support to assist in returning the storage device to the previous functioning state.

MANAGED WORKSTATION

WINDOWS WORKSTATION SUPPORT

Windows Workstation Operating System Support includes remote support to return the Operating System to the previous functioning state and patching of the Operating System.

MAC WORKSTATION SUPPORT

Mac Workstation Operating System Support includes remote support to return the Operating System to the previous functioning state.

ANTIVIRUS

Company offers real-time antivirus threat protection with built in remediation.

MICROSOFT OFFICE SUITE TROUBLESHOOTING

Microsoft Office Suite products include, but is not limited to Outlook, Word, Excel, PowerPoint, and other applications depending on license type. Company will install licensed software and provide remote troubleshooting support for errors and issues related to functionality of these products.

OFFICE 365 MANAGEMENT

Company will assist in remote management of Customer's Microsoft Office 365 environment, including user and license management. Services include adds, changes and deletions of users, password resets, email routing, rule management, assistance with licensing questions, etc..

HARDWARE FAULTS

Company will assess hardware failures on covered devices and facilitate repair or replacement by the hardware vendor. The Customer will maintain hardware warranties or provide timely payment for repair charges for any Customer provided equipment covered under the SOW, and pay for any costs associated with required upgrades, maintenance agreements, to address any new features or security concerns.

WARRANTY MANAGEMENT

Company will assist customer in tracking hardware and software contract expiration dates to allow for timely renewal of support or replacement of the covered product.

WINDOWS WORKSTATION PATCHING

Company approves routine patches from Microsoft, that are applied to Workstations on a weekly cadence to minimize vulnerabilities and risk.

Company suggested patching schedules and policies are available upon request.

MANAGED DATA PROTECTION

LOCAL/CLOUD BACKUP

Our Local/Cloud Backup data protection solution is scheduled to have nightly local and cloud-based backups, if applicable, and a retention period of at least 30 days, if possible. In the event of a failure, the data protection team will remediate and reschedule jobs to reduce the potential for data loss as much as possible. Backup device is sized based on Company best practices.

LOCAL/CLOUD BACKUP AND CONTINUITY

Our Local/Cloud Continuity data protection solution includes all features of our Local/Cloud Backup solution, with the added option to run an instance of your server on the local backup appliance or in a cloud environment.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING ("BCDR")

Our BCDR offering provides the plan that the Customer and Company will be able to execute in the event of a declared disaster. For full disaster recovery capability to be understood a formal project would be required to assess the processes and technical needs that would be administered by Customer with assistance from Company. Full disaster recovery is not guaranteed or included in the price. Testing of the DR Plan and other Services provided in conjunction with the DR plan will be provided on a Time & Materials basis.

MANAGED NETWORK AND MANAGED OTHER DEVICE ON NETWORK

ESSENTIAL MONITORING

Company will monitor all supported devices using a standardized monitoring and alerting process for critical services as needed. Automated recovery options are used where appropriate, otherwise remote remediation will be completed by Company.

DEVICE SUPPORT

Network and Other Device support includes remote support to return the device to the previous functioning state.

PATCHING

Patching for other devices, such as Firewalls, Switches, Wireless Access Points, ESXi Servers, etc., while not included in this SOW, can be conducted on a Time & Materials basis, or may be covered under the Enhanced Monitoring, Notification and Reporting service.

ENHANCED MONITORING, NOTIFICATION AND REPORTING

Customer's Managed Server, Network and Other Device on Network is monitored remotely with an automated notification system for issues or seriously adverse trends related to availability or performance.

Dashboards provided through the Customer Portal provide visibility into the performance, capacity, and availability of Customer's technology.

Updates and security patches for Managed Network devices that are covered by Enhanced Monitoring, Notification and Reporting that may be performed remotely are included and may be performed upon request of Customer. Company policy on update and security patching is available upon request.

EMAIL SECURITY/SPAM FILTERING

SECURITY – SPAM FILTERING/THREAT PROTECTION/ENCRYPTION

The "Security" Email Protection level includes inbound and outboard protection, which combines behavioral, heuristic, and sandboxing technologies to protect against zero hour and targeted attacks.

COMPLETE – SECURITY PLUS ARCHIVING/BACKUP

The "Complete" Email Protection level includes all the features of "Security" and adds cloud-to-cloud compliance archiving and backup of Office 365 data.

TOTAL – COMPLETE PLUS AI/HEURISTICS/PHISHING TRAINING

The Total Email Protection package includes all the features of "Complete" plus advanced forensics, end-user phishing training, and artificial intelligence to detect advanced spear-phishing attempts.

PHISHING TRAINING

Phishing training provides an automated platform to deliver suspicious email campaigns to identify end users requiring additional anti-phishing training.

FOLLOW ME FILTERING

FOLLOW ME FILTERING (DNS BASED)

Follow me filtering for workstations blocks requests to malware, ransomware, phishing, and botnets before a connection is even established — stopping threats over any port or protocol before they reach the network or endpoints.

MULTIFACTOR AUTHENTICATION

Multifactor authentication may be provided for supported providers. Implementation of multifactor authentication may require a project.

COMMUNITY PORTAL ACCESS

FULL LIFECYCLE CASE TRACKING AND REPORTING

Case logging, tracking, communication, escalation (as required), closure, and reporting are performed using Company's Case Management system. Customer Portal access is provided, enabling secure review of open and closed Cases, submission of new Cases, and other capabilities.

CLIENT EXPERIENCE

IT STRATEGY BUSINESS REVIEWS

All Managed IT customers will regularly meet with their dedicated Client Experience team member. They will help align the business and technical strategy with our customers and the support team. They will also help with road mapping and planning for future needs, including budget planning and identify and business risks existing or foreseen based on the business roadmap of the customer.

FULL LIFECYCLE CASE TRACKING AND REPORTING

Case logging, tracking, communication, escalation (as required), closure, and reporting are performed using Company's Case Management system. Customer Portal access can be provided through an optional Community Portal license, enabling secure review of open and closed Cases, submission of new Cases, and other capabilities. Hardware and Software Inventory Reports can also be used to ensure alignment with technology needs.

NETWORK ADMIN

IDENTIFY TRENDS AND TECHNICAL RISKS

The Network Administrator function is performed by a dedicated Company Engineer to maintain consistency and familiarity with Customer's environment. They conduct remote reviews of the infrastructure and identify any risks and trends based on the information the tools are exposing or potential issues that are identified via a visual inspection.

DEVELOP AND MAINTAINS TECHNICAL DOCUMENTATION

After the onboarding project, Company documents Customer's environment and periodically reviews and updates the documentation. These documents are stored in Company's systems for reference by Company or Customer. Any privileged password information is stored in a password vault, where Company tracks who has accessed this information. This plays a vital role in Company's ability to regularly change privileged passwords or initiate changes upon employee termination.

SERVICE LEVEL AGREEMENTS (SLA)

Case Response: For Covered Components, the Initial Response SLA for Cases is defined by the following table. Initial Response denotes engagement by a Company engineer. For the SLA to apply, the Client is required to contact the service desk (via the phone number, e-mail, or Case Management system via the Community Portal):

Case Priority	Response SLA*	Definition
Critical (P1)**	15 Minutes	Impacts the majority of end users company-wide - and either - Causes complete inability to conduct business, or significant safety or security risk; or No workaround available and immediate resolution or workaround is required
High (P2)**	1 Extended Business Hour	Impacts ability to conduct normal business operations without a workaround; or Critical Case with temporary workaround
Medium (P3)	8 Extended Business Hours	Resolution important but not required immediately; or End user moves, adds or changes, include ordering and setup of new and existing computer hardware
Low (P4)	24 Extended Business Hours	Minimal business impact; or Preventative maintenance; or General inquiries (e.g., end user training, questions)
Planning	Variable	Enhancement

**Denotes elapsed service hours. For P1s this is 24x7 or 8x5 depending on coverage level, and for P2s through P4s this is 8x5.*

***For this Response SLA to apply, Critical (P1) and High (P2) Cases require call to the service desk*

WORK PREREQUISITES

The Work Prerequisites for services under this SOW are:

- A fully executed IT Master Services Agreement.
- Company must receive one original copy of this document with an authorized signature. Upon receipt, this project will commence with Customer on-boarding for the managed services requested on a mutually agreed upon timeline.
- If any written authorization form is required to perform testing, Company will provide the required form to Customer.
- Customer must designate a single point of contact and a backup contact for communications with Company personnel.

CUSTOMER RESPONSIBILITIES

- Customer must maintain a business class firewall at each location with static IPs.
- Customer must have appropriate business class internet speeds. Requirements are higher for offsite backups.

- Customer must maintain a warranty for all hardware being supported.
- Customer must have and maintain support agreements for all supported applications and operating systems.
- Customer must provide any application or hardware licensing and related information upon request.
- All hardware and software solutions must be properly sized for their intended use.
- All hardware, software and services that will be supported by this SOW must be included in the IT Service Catalog. Any exceptions must be remediated concurrent to onboarding.
- Customer must allow Company reasonable access and support maintenance windows.
- Company must have access to Customer's systems during normal business hours.
- Customer must provide a primary and secondary designated point of contact for billing, security/access and technical related issues (this need not be the same contact).
- Workstations and Servers must be turned on during their Scheduled patching windows.
- Customer must contact Company by phone with any Priority 1 or 2 issues. All other issues can be submitted via phone, email or on-line.
- Customer is responsible for their data. Data needs classified and secured appropriately via user and group permissions to volumes, shares, and folders.
- Customer should not modify or uninstall any hardware or software necessary for Company to monitor or support Customer.
- Customer will inform Company of any 3rd party patching requirements and sign off on the schedule and implementation of it.
- Customer must provide IT personnel to assist with remote troubleshooting, as needed.
- Customer's users must be available during troubleshooting client issues unless otherwise directed by Company personnel.
- Company is not responsible for Customer data or any loss of data resulting directly or indirectly from this SOW.

VENDOR MANAGEMENT - APPLICATION/SYSTEMS SUPPORT

Company will act as a liaison with vendors to support the applications and systems as identified in this SOW. Customer must have a current support agreement in place with all the identified vendors for the duration of the contract terms of this SOW. Support for these applications and systems will be initiated by Customer, however, Company may contact the vendor if technical expertise is required. At times the vendor and Company may require assistance from an IT point of contact at the Customer's site; Customer must provide reasonable assistance when necessary. The Customer is responsible for the development, installation, configuration, maintenance, patching, upgrade, troubleshooting and security of their business software. Any assistance requested from Company IT required to meet these obligations may involve a charge rate

SUPPLEMENTAL BILLING DETAIL

HARDWARE RELEASE AND INVOICING TERMS

All hardware, software, and support contracts on the associated Sales Order(s) are authorized for immediate invoicing upon receipt of shipment to the Customer's shipping address provided on the Sales Order(s). The Customer agrees to fund the invoice within Company's approved account receivable terms and will remit payment via an approved payment vehicle.

Furthermore, the Customer understands this does not include any service fees rendered through Company, and that all service charges will be accrued as agreed upon via this Statement of Work or Professional Services Estimates to be paid upon milestone or progression billing by calendar month. Please see Pricing in the Summary section for more details.

SUPPORT CALLS

This service provides resolution of Customer IT related issues. Requests may be initiated by email or phone. Customers may reach out for support via email at XIT-ManagedServices@Xerox.com and by phone at 1-877-XEROXIT.

STATEMENT OF WORK CHANGES AND/OR ADDITIONS

Company offers a wide variety of consulting services. We will partner with your Company to help you meet every business objective possible. Please make us aware of any changes and/or additions to this SOW or to your business needs. Upon identification of potential scope changes, Customer and Company will agree on the course of action. As appropriate, Company will then proceed to generate a new SOW or Change Request Form.

EXECUTION

Company believes the SOW outlined in this document will meet the requirements of the work to be performed. Any modifications to this document will be made in writing and agreed to by both parties and may be subject to additional charges.

City Of Prairie City	RK Dixon a Xerox Company
Printed Name	Printed Name
Signature	Signature
Date	Date

MARCO IT SERVICES CONTRACTS

	Managed IT	Premium IT	Billable IT
Procurement	Monthly Per User Unlimited Use – No Overage Billing	Monthly Fee (Min. $1000) Billed Consumption w/Rollover	Billed for Time and Materials
Contact Methods	800.847.3097 MIT@marconet.com	800.847.3098 ITservice@marconet.com	800.847.3098 ITservice@marconet.com
Service Teams	Rapid Resolution (Triage and Remediation); CARE Team; Network Specialists; Field Services	Rapid Resolution (Triage Only); IT Remote Support Team; Field Services	Schedule Field Services
Support Availability *24x7x365 Uplift Available**	Triage: 24x7x365 Remediation: M-F: 8am - 5pm CST*	Triage: 8x5xNBD Remediation: M-F: 8am - 5pm CST	Triage: 8x5xNBD Remediation: M-F: 8am - 5pm CST
Service Level Targets *(Response Time)*	Priority One - 7 minutes Priority Two - 7 minutes Priority Three - 10 Minutes	Priority One - 30 minutes Priority Two - 60 minutes Priority Three - 90 Minutes	
Documentation	Dynamic Documentation	Static Documentation	
Call Center Handling	Live-Call Answer Warm Transfer to CARE Team	Live-Call Answer Urgent Issue Transfer + Call Back	Schedule Call Back

Onsite Service Inclusion	Recurring Maintenance;
	Recurring Health Checks;
	Escalation to Field Services		

Recurring Business Reviews	Client Sales Associate		
Managed Backup	Eligible for Managed Backup		
Monitoring	24x7x365 Alert Monitoring		
Patch Management	Microsoft and 3rd Party**		

Managed Tools Services Included	Monitoring and Patching Agent;
	Remote Management Agent;
	Anti-Virus and Anti-Malware;
	Email SPAM Security;
	Content Security
	End-User Security Training;
	Lifecycle Management Reporting		

Service Onboarding	Installation of Management Tools and Services; Environment Documentation	Environment Documentation	

GET STARTED TODAY

800.847.3098
marco@marconet.com

marco®

taking technology further

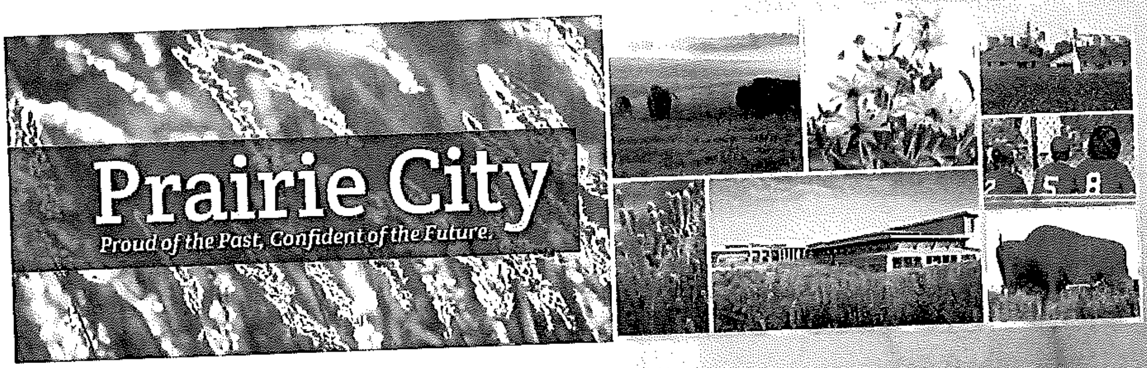
marconet.com

BUSINESS IT • MANAGED SERVICES • CLOUD SERVICES • COPIERS & PRINTERS

All Covered
IT SERVICES FROM KONICA MINOLTA

MMIT
PROFESSIONAL SERVICES

MMIT Business Solutions Group & All Covered Care Proposal and Schedule of Services for



Prepared by:

Justin Perry, MMIT Business Solutions Group

Michael O'Crowley, Strategic Account Manager, All Covered

5/3/2022

Pricing is valid for 15 days from the date of this document
Confidential and not to be distributed to third parties

KONICA MINOLTA

March 30, 2022

Dear Jodie,

Thank you for considering MMIT Business Solutions Group / All Covered as City of Prairie City IT support partner. We strategically built a comprehensive IT support model that is unique in the marketplace. As an established, local family business, MMIT Business Solutions Group has been supporting Des Moines Area organizations for the past 85 years. In addition to our extensive IT knowledge and talent, our strategic partnership with All Covered (AC) has enabled us to bring additional expertise, experience and bandwidth to help support our client's various IT needs.

Our Managed Network Services (MNS) programs take a "pro-active" approach to IT

support. Instead of the traditional support model of "reacting" when there are IT related issues, we've proven that by monitoring and managing our client's infrastructure 24/7 and doing remote triage when appropriate, we can "pro-actively" get in front of the majority of IT related

issues. Additionally, our comprehensive program includes detailed IT documentation (Guide Book), IT consulting / budgeting and tier 1,2 & 3 US based Help Desk support.

My goal is to build a long-term, mutually beneficial partnership between City of Prairie City and MMIT / AC. In addition to providing world-class technology and local, award-winning services, you will find three main attributes of MMIT Business Solutions Group to be different that any vendor in this competitive marketplace.

Accountability: MMIT Business Solutions Group is 100% responsible and accountable for our valued customers. We are empowered to make quick, customer-focused decisions without any corporate bureaucracy. We own all aspects of our vital customer relationships.

Vested Interest: As a family business, we truly have a vested interest in our client's long-term satisfaction. Unlike other organizations where the representatives and managers often change, the partners of MMIT Business Solutions Group have a vested interest in customer satisfaction not only on day one or year three - we want to keep our customer's for life!

Unique "Value-Add" Programs: Instead of simply providing IT support, MMIT Business Solutions Group / All Covered are constantly looking for ways to help our customers: reduce costs, budget accurately, improve efficiencies and solve problems. As a Managed IT and Output Services company, we customize programs to help customers where they need it – including providing world-class multi-function platforms, robust Content Management / Electronic Workflow solutions, comprehensive Managed Network IT Support programs to helping with one time to IT projects.

Thank you again for the opportunity to earn City of Prairie City business. I am confident, after you review the following proposal, you will feel MMIT Business Solutions Group / All Covered will bring the most value as a business partner to City of Prairie City.

STATEMENT OF NEED

City of Prairie City is looking for managed IT services partner that can help them address the need for 24x7x365 access to helpdesk servie

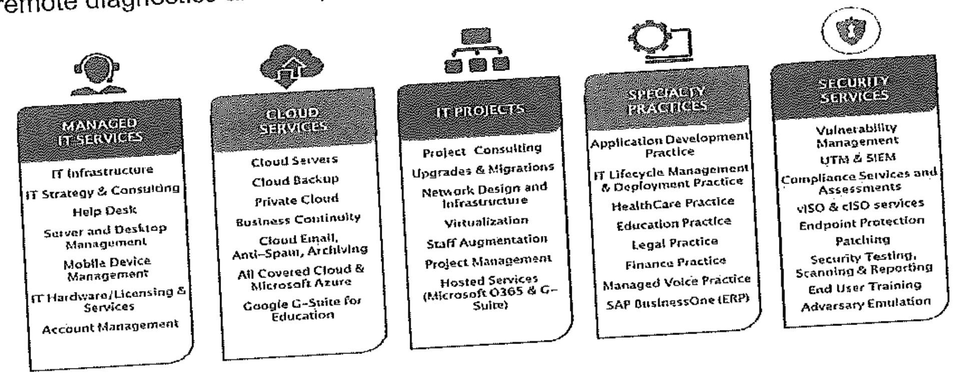
BENEFITS OF MMIT BUSINESS SOLUTIONS GROUP & ALL COVERED SOLUTION

All Covered Care (ACC) is designed to increase each client's return on technology investments by creating and supporting a stable and secure IT infrastructure, tuned to the client's business needs. Through a strong partnership with the client, MMIT & AC team delivers proactive and preventive PC, Network and Server management, troubleshooting and user support, backed by documentation and planning. MMIT & AC also offers a range of Cloud Server, Hosting, Security and Application Development services.

Experience has shown that regularly scheduled management of systems and networks will substantially reduce the frequency and severity of the common problems that jeopardize the stability, security, and performance of an organization's IT environment.

ACC is delivered through a combination of remote and on-site services.

- **Proactive Services and Preventive Support.** These remote services are based on a proven methodology that will help the IT environment run smoothly and prevent many problems before they affect computer or network performance.
- **Monitoring and Reactive Support.** Support initiated by either party provides response to active issues. Troubleshooting and problem-solving are provided on-site if appropriate. The managed environment is monitored 24 hours a day.
- **End-user Support.** This addresses day-to-day end-user problems primarily through remote diagnostics and telephone support.



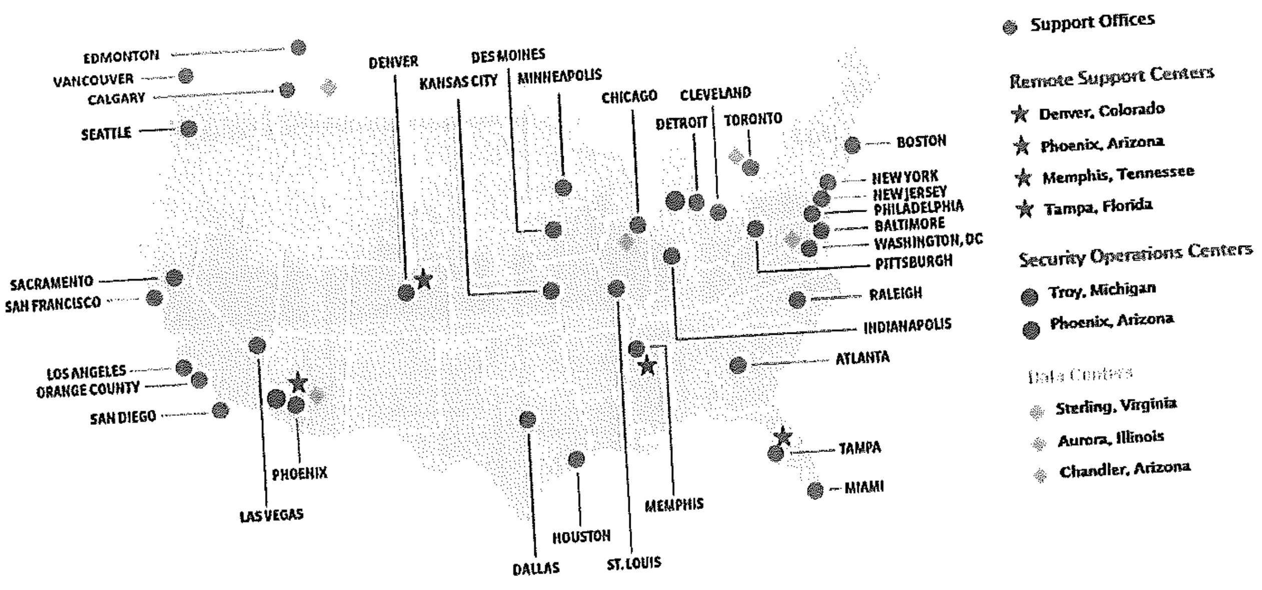
MANAGED IT SERVICES	CLOUD SERVICES	IT PROJECTS	SPECIALTY PRACTICES	SECURITY SERVICES
IT Infrastructure	Cloud Servers	Project Consulting	Application Development Practice	Vulnerability Management
IT Strategy & Consulting	Cloud Backup	Upgrades & Migrations	IT Lifecycle Management & Deployment Practice	UTM & SIEM
Help Desk	Private Cloud	Network Design and Infrastructure	HealthCare Practice	Compliance Services and Assessments
Server and Desktop Management	Business Continuity	Virtualization	Education Practice	vISO & cISO services
Mobile Device Management	Cloud Email, Anti-Spam, Archiving	Staff Augmentation	Legal Practice	Endpoint Protection
IT Hardware/Licensing & Services	All Covered Cloud & Microsoft Azure	Project Management	Finance Practice	Patching
Account Management	Google G-Suite for Education	Hosted Services (Microsoft O365 & G-Suite)	Managed Voice Practice	Security Testing, Scanning & Reporting
			SAP BusinessOne (ERP)	End User Training
				Adversary Emulation

MMIT Business Solutions Group & All Covered Care Engagement Plan For City of Prairie City

ON-BOARDING PROCESS

- A kick-off meeting will be held to introduce the details of the support model to you and to officially begin the startup phase.
- Your support team will include Service Delivery Engineers, their managers, an Account Manager, a Project Coordinator, and a representative from Operations.
- The environment will be fully documented in an electronic guidebook
- Remote monitoring is set up for key network elements by our Managed Services team. MMIT Business Solutions Group & All Covered Service Desk then monitors these network elements. The Service Desk operates 24 hours a day, staffed with MMIT Business Solutions Group & All Covered employees, and performs round-the-clock monitoring of critical devices and applications with alarm conditions being validated, remediated and escalated to your service delivery team as needed.
- Support is available to you starting on the effective date of the contract. Urgent needs are communicated by calling MMIT Business Solutions Group & All Covered Service Desk.

SUPPORT LOCATIONS



ON-GOING SUPPORT

- MMIT Business Solutions Group & All Covered team will manage the network, servers, computers and technology infrastructure based on a comprehensive support plan.
- Proactive management of the systems helps to avoid problems that would otherwise interfere with day-to-day operations.
- End user problems are addressed promptly and the systems are monitored continuously to ensure rapid response to emerging issues.
- MMIT Business Solutions Group & All Covered manages escalations to your telecom service providers, hardware vendors, software vendors and application providers.
- Upon request, MMIT Business Solutions Group & All Covered will act as support-liaison for end-user to initiate a support call to Line of Business support provider and request support on behalf of end-user and direct vendor support provider to work directly with end-user to resolve issue.

SERVICES NOT INCLUDED

- Services not specifically defined in this agreement are excluded from it, such as, but not limited to the following. These services may be available as separately billed projects.
  - Programming and Line of business application support
  - Software and hardware upgrades, cabling
  - Home or private network troubleshooting
  - Audio/visual support (projectors, TVs, etc.)
  - New application, computer, or peripheral installations
- MMIT & All Covered do not provide hardware repair and recommends Client uses warranty or vendor repair service

SYSTEM REQUIREMENTS

The full and effective operation of MMIT & All Covered's service delivery tools and processes depend on the following system requirements being met. Requirements that are not met may affect system stability and the ability for MMIT& All Covered to resolve issues promptly.

- Servers:
  - Servers must be from a major brand (Dell, Cisco, HP, IBM, Lenovo, etc.)
  - Servers must be under current manufacturer hardware warranty or manufacturer hardware maintenance contract
  - Servers must have an appropriate amount of memory for the applications to function properly
  - Hardware Management Cards for servers must be installed and licensed fully
  - Servers must be connected to a managed/smart UPS backup
- Firewall:
  - Firewalls must be from a major brand (Cisco, Fortinet, SonicWall, etc.)
  - Firewalls must be a current/supported model

    - Firewalls must be under manufacturer warranty
    - Firewalls must have relevant support contracts
    - Firewalls must have a static public IP address
- Support will not be provided for any operating system, application, or device that is beyond the manufacturer's published End of Support date.
- All systems must be backed up using an All Covered managed, or industry-standard backup solution.
- Ethernet cabling must be Category 5E or higher and be properly grounded and bonded.
- Suitable power surge protection must be installed for all critical systems.
- Room temperature must be maintained for servers and network devices according to manufacturers' specifications.
- All Client servers and computers must be covered under the Schedule of Services unless specifically agreed to therein.

CLIENT REQUIREMENTS

Client agrees to:

- Implement safe browsing and safe email procedures and best practices. No anti-virus solution is foolproof and Client's systems are not guaranteed to be 100% virus free by using any anti-virus solution.
- Provide remote access to all supported devices to allow technical issues to be resolved.
- Notify MMIT & All Covered via Service Ticket twenty-four (24) hours or more prior to any significant proposed device changes for non-system down issues to allow MMIT & All Covered to review prior to any changes occurring.
- Own genuine user or device licenses for every operating system and application installed and to maintain records of all software media with CD-keys, serial numbers and unlock codes.
- Own valid maintenance contracts for all software and devices and to designate MMIT & All Covered as an authorized agent of Client under those contracts.
- Maintain third party software support contracts for all line-of-business applications to address end-user support, updates and upgrades, or to maintain expertise internally by Client's staff.
- Designate a primary point of contact or contacts to interact with the Help Desk to avoid multiple tickets being generated for the same issue and to perform simple, guided on-site tasks.
- Plan for the upgrade of any device, operating system or application that is scheduled to become end-of-support by its manufacturer; whether or not covered under the Schedule of Services.