

Managed Agreement Terms

Active IT Managed Agreement between NETWORK PEOPLE, LLC. (NETWORK PEOPLE) referred to as "NETWORK PEOPLE" and CITY OF MADEIRA BEACH, referred to as "COMPANY". Agreement includes a proposal document with a signature page and fee structure included herein as EXHIBIT A. Once executed by both parties, this Agreement shall be effective as of the Signing Date.

NETWORK PEOPLE will commence service under the terms of this agreement only after it receives and accepts this Agreement signed by a COMPANY authorized representative.

0.0 Agreement and Term will commence on the date that both parties have executed this agreement and the Effective Start date of delivery of services commences on said date. Effective Start Date may be delayed if necessary by one or more parties depending on logistics but commencement will not be delayed more than 30 days from when both parties have signed. The Effective Start Date (day both parties sign) as listed on this Agreement shall remain in effect for the entire Term of the agreement not to exceed 5 years (a total of 60 months). The agreement will automatically renew for additional periods of the same length as the initial Term unless one party provides the other party a written notice that is terminating the Agreement not more than 90 days and not less than 30 days prior to end of the Contract Term specified in the Agreement.

0.1 Onboarding Phase is required for all new Service Agreements and will be scheduled at time of signing. This phase will precede the **Active IT Managed** start date by two weeks. Once onboarding phase is complete, **Active IT Managed** support services will commence. If service start date does not fall on the 1st of the month, cost of service will be prorated for the month according to actual start date.

0.2 Provisions for other Agencies. Unless otherwise stipulated, NETWORK PEOPLE agrees to make available to all "Eligible Users" the prices submitted in accordance with the terms and conditions of the contract resulting from this solicitation. Eligible Users means all State of Florida government agencies, the legislative and judicial branches, and political subdivisions (counties, local district school boards, community colleges, municipalities, or other public agencies or authorities), which may desire to purchase under the terms and conditions of this resulting agreement.

1. Service Fees and Billing.

COMPANY agrees to pay the recurring charges for Service as identified in EXHIBIT A, as well as the hourly service rate for time required beyond the services covered by the agreement. Service charges may not include applicable taxes (if any), shipping charges (if any), or remediation charges, all of which shall be billed in addition to the Service Charges (or billed by third party providers) and shall be the responsibility of the COMPANY to pay in full. Once payment is made on any and all services, there are absolutely no refunds.

1.1. Initial Payment. NETWORK PEOPLE will charge COMPANY for onboarding fees, and any hardware costs at time of signing. Upon COMPANY acceptance and full execution of this Agreement, the amount will be due in full.

1.2. Remediation. Remediation and Security Incident Remediation. Remediation by NETWORK PEOPLE will be billed hourly if determined a project or cyber security remediation. If remediation is required after hours, then COMPANY will be billed at the afterhours rate. NETWORK PEOPLE will work additional hours upon the COMPANY's request at the rates detailed under "Service Response and Rates" section. A cyber security insurance policy is highly recommended with a minimum of 1 million dollars in coverage. If COMPANY suffers a cyber security incident, the cyber security insurance is a critical tool to cover expenses such as security incident response and remediation, loss of business income, public relations damage, payment in bitcoin, negotiations with hackers, and legal advice, etc.

1.3. Recurring Charges. NETWORK PEOPLE will bill COMPANY monthly in advance for Managed Services being provided under this Agreement. If service start date does not fall on the 1st of the month, cost of service will be prorated for the first month according to actual start date.

1.3.1 Agreement Adjustments. To ensure your inventory is correct and your devices are safe, NETWORK PEOPLE will perform a monthly audit of all devices and products (this includes licenses) for your environment. In the event there are additional devices or products needed, or devices and products have been removed, the service agreement will be adjusted up/down accordingly to support the environment. This audit will happen on the 15th of the month and it is the COMPANY's responsibility to inform NETWORK PEOPLE of any changes they see needed by the 25th of the month. This applies to the current month's billing. Previous invoices will not be adjusted or issued a credit. NETWORK PEOPLE will automatically retire devices after a 30 day stale window and adjust support products and licenses as well, in tandem. This ensures that the COMPANY is only charged for what NETWORK PEOPLE is supporting, and the environment stays protected.

1.4. Payment for Services. All Service Charges and other fees will be due in U.S. dollars on the 1st day of every month. If payment for the current month is not received by the 15th of that month, a fee equal to the greater of \$35.00 or 5% of that month's Active IT Agreement will be assessed and services may be suspended until the late payment is received. Late payments will also accrue interest at a rate of eighteen percent (18%). If payment is returned to NETWORK PEOPLE with insufficient funds, COMPANY is considered to not have paid and subject to a returned check charge of \$50 and service may be suspended. COMPANY understands that any Federal, State or Local Taxes applicable shall be added to each invoice for services or materials rendered under this Agreement. COMPANY shall pay any such taxes unless a valid exemption certificate is furnished to NETWORK PEOPLE for the state of use.

1.4.1 Nonpayment & Cancellation Fee. NETWORK PEOPLE may suspend Service to COMPANY if any amount due hereunder is not paid in full within fifteen (15) days after COMPANY is sent an overdue notice. To reinstate Service, NETWORK PEOPLE will charge a service fee of \$500.00. NETWORK PEOPLE may suspend service on this Agreement if any amount due hereunder is not paid in full within thirty (30) days after COMPANY is sent an overdue notice. COMPANY agrees to pay for full amount of the monthly service even if NETWORK PEOPLE has to suspend service for part of that month due to non-payment. If COMPANY fails to pay any overdue balance, NETWORK PEOPLE will at its discretion hold any equipment owned by COMPANY until fees are paid in full or at its discretion prevent access to services provided.

1.5. Payment for Work Outside the Scope. COMPANY understands that any and all Services, hardware or software requested by COMPANY that fall outside of the terms of this Agreement will be considered Work Outside the Scope of this Agreement. Any Work Outside the Scope of this Agreement will be billed separately and due upon receipt of services.

1.6. Rate. COMPANY understands the rate will be "locked-in" for the first 12 months then increase by a COLA of 5% every year thereafter to compensate for the cost of inflation and annual price increases from our vendors.

2. Services and Tools.

2.1. Covered Services. NETWORK PEOPLE will provide service for items listed in the "Monthly Expense Summary" for the benefit of the COMPANY as part of this Agreement.

2.2. Work Outside the Scope. NETWORK PEOPLE may invoice COMPANY for Work Outside the Scope of this Agreement at the rate stated under the COMPANY'S "Service Response and Rates" section. Out of scope work includes but is not limited to troubleshooting, diagnosing, repairing, configuring of computers, mobile devices, or servers/printers/NOC equipment that is NOT Itemized and paid for under this support agreement. In other words, if equipment is not covered under the Active IT Managed Agreement, it will not be supported. However, in instances where the COMPANY needs to replace equipment under their Active IT Managed Agreement, COMPANY agrees that if the product is purchased through NETWORK PEOPLE, NETWORK PEOPLE will add the equipment onto the network free of charge and it will then be added to Active IT Managed Agreement. If the COMPANY purchases the product from a different vendor, COMPANY will be charged the going rate as stated in the "Service Response and Rates" section.

2.2.1. Travel Time. Travel between NETWORK PEOPLE'S site and the COMPANY site will be subject to an hourly rate as listed under "Service Response and Rates" if travel is beyond Pinellas, Pasco, and Hillsborough counties.

2.2.2. Meals and Lodging. Daily meals and lodging may be billed to the COMPANY if services require travel of more than 50 miles from the NETWORK PEOPLE headquarters. Amount billed per day for meals and lodging will be charged at the following dollar amounts: standard hotel room near office if engineer needs to stay overnight and per diem of \$65 for meals per engineer.

2.3. Service Hours and Rates. Please reference <https://www.networkpeople.com/sla-response-and-rates/> for Service Level Agreement, Hours of Operation, and Rates. All Work Outside the Scope of this Agreement or Project work will be billed under the provisions under the RATES section."

2.4. Response/Resolution Times and Service Levels. NETWORK PEOPLE response time will be handled in accordance with the provisions detailed under the section "Service Response and Rates."

2.5. Support and Escalation. NETWORK PEOPLE will respond to COMPANY'S Tickets as quickly as possible but not to exceed response times noted in "Service Response and Rates." Tickets can be opened using the following and each incident will be assigned a ticket number for tracking:

1. a) By telephone using (727) 446-4564, option 1 for Dispatch Center; or
2. b) Via email to our Dispatch Center; ticket@NetworkPeople.com

2.6. Facility Access. NETWORK PEOPLE will need access to the COMPANY facility during normal business hours and may need access afterhours for emergency and afterhours work. Facility access will also include a work area and a meeting area for use during the duration of this Agreement. If business hour access is not granted to NETWORK PEOPLE, COMPANY will not hold NETWORK PEOPLE responsible for any missed deadlines, missed milestone dates, or failure to provide required Service Level Agreement (SLA) times.

2.7. Chronically Failing Equipment. Experience has shown that equipment belonging to the COMPANY which initially passed the Minimum Standard Requirements for Service can become chronically failing. This means that the equipment repeatedly breaks down and consistently causes user and business interruption even though repairs are accomplished. Should this occur, while rare, COMPANY agrees to work constructively and positively with NETWORK PEOPLE to replace the equipment at additional cost to the COMPANY.

2.8. NETWORK PEOPLE Equipment. COMPANY agrees that any Equipment specified as NETWORK PEOPLE Equipment, will remain the sole property of NETWORK PEOPLE with security interest and COMPANY will not attempt to sale, resale, tamper, troubleshoot, repair, move, add, etc. to this Equipment without verbal or written permission of NETWORK PEOPLE. Should this contract terminate by either party, COMPANY agrees to return the Equipment to NETWORK PEOPLE within 30 days from the final cancellation date. COMPANY further acknowledges and gives permission to NETWORK PEOPLE to seize Equipment from location in event of contract termination after 30 day grace period, and agrees to compensate NETWORK PEOPLE for all expenses accrued during the seizure process. In the event of termination of this contract, COMPANY will be given the option of purchasing any NETWORK PEOPLE owned equipment at a fair market value to be determined at that time. COMPANY agrees to make all logical and earnest attempts to keep equipment safe, secure and protected while in their possession. Should COMPANY default on this agreement, permission is granted to enter their premises at any time and remove all of NETWORK PEOPLE'S hardware, and all efforts to recover such property will be deemed consensual and not a trespass.

2.9. Change Management Process. The following processes will be followed for any change of scope request: 1. Problem Identification, 2. Delivery of Change Request, 3. Logging of Change Request, 4. Approval and Acceptance, 5. Implementation.

3. Disclaimer of Third Party Actions and Control

3.1 Disclaimer of Third Party Actions and Control. NETWORK PEOPLE does not and cannot control the flow of data to or from the network and other portions of the Internet. Such flow depends in large part on the performance of Internet services provided or controlled by third parties. At times, actions or inactions caused by these third parties can produce

situations in which COMPANY connections to the Internet (or portions thereof) may be impaired or disrupted. NETWORK PEOPLE cannot guarantee that such situations will not occur and, accordingly, NETWORK PEOPLE disclaims any and all liability resulting from or related to such events.

4. Limitations of Liability.

4.1. Personal Injury. NETWORK PEOPLE will not be liable for any harm or personal injury to COMPANY personnel resulting from any cause, other than NETWORK PEOPLE'S gross negligence or willful misconduct.

4.2. Damage to COMPANY Equipment. NETWORK PEOPLE is not liable for damage to, or loss of any COMPANY Equipment resulting from any cause, other than NETWORK PEOPLE'S gross negligence or willful misconduct and then only in an amount not to exceed the replacement value of the damaged COMPANY Equipment, or the total amount paid by COMPANY to NETWORK PEOPLE.

4.3. Damage to COMPANY Business. In no event will NETWORK PEOPLE be liable for any incidental, punitive, indirect, or consequential damages (including without limitation any lost revenue or lost profits) or for any loss of technology, loss of data, or interruption or loss of use of Service or any other similar claims by COMPANY or related to COMPANY'S business, even if NETWORK PEOPLE is advised of the possibility of such damages. NETWORK PEOPLE will not be liable for any damages or expenses incurred by COMPANY as a result of any deficiency, error, or defect in NETWORK PEOPLE'S service whether due to equipment, hardware, software, or NETWORK PEOPLE'S failure to correct the same, except in the event of NETWORK PEOPLE'S willful actions and only to the extent that such damages are covered by NETWORK PEOPLE insurance in which NETWORK PEOPLE shall provide the COMPANY a current copy of its insurance declaration page.

4.4. Maximum Liability. Notwithstanding anything to the contrary in this Agreement, NETWORK PEOPLE'S maximum aggregate liability to COMPANY related to or in connection with this Agreement whether under theory of contract, tort (including negligence), strict liability or otherwise will be limited to the total amount paid by COMPANY to NETWORK PEOPLE.

5. No warranty.

Except as specifically set forth herein, the services are provided on an "as is" basis. Network People does not make, and hereby disclaims, any and all other express and implied warranties, including, but not limited, warranties of merchantability, fitness for a particular purpose, noninfringement and title, and any warranties arising from a course of dealing, usage, or trade practice. Network People does not warrant that the services will be uninterrupted, error-free, or completely secure.

6. Indemnification.

6.1. By COMPANY. In no event shall NETWORK PEOPLE be liable for any special, indirect, consequential, or punitive damages to COMPANY or any other party as a result of the performance or non-performance by Network People, Inc. of any services described herein, (including, without limitation, loss of data, profits, or use of software) whether foreseeable or not, even if Network People, Inc. has been advised of the possibility of such damages. Network People, Inc.'s liability with respect to, arising from, or in connection with this agreement, whether in contract, in tort, or otherwise, is limited to amounts paid by The Company to Network People, Inc., excluding travel and per diem expenses, pursuant to the terms hereof.

6.2. By Network People. If NETWORK PEOPLE'S equipment is located at COMPANY'S office or data center, NETWORK PEOPLE will indemnify, defend and hold harmless COMPANY, its directors, officers, employees, affiliates and companies (collectively, the "Customer Covered Entities") from and against any and all claims, actions or demands brought against any of the Customer Covered Entities alleging (a) with respect to the COMPANY'S business: (i) infringement or misappropriation of any intellectual property rights; (ii) defamation, libel, slander, obscenity, pornography, or violation of the rights of privacy or publicity; or (iii) spamming or any other offensive, harassing or illegal conduct or violation of the Acceptable Use Guidelines; (b) any loss suffered by, damage to or injury of any other NETWORK PEOPLE'S COMPANY, any other NETWORK PEOPLE'S equipment or any other NETWORK PEOPLE'S representatives, employees or agents, which

loss, damage or injury is caused by or otherwise results from acts or omissions NETWORK PEOPLE, its representative(s) or its designees; (c) any personal injury suffered by any NETWORK PEOPLE. personnel arising out of such individual's activities related to the Services, unless such injury is caused by COMPANYS' negligence or willful misconduct; or (c) any other damage arising from the NETWORK PEOPLE'S Equipment or NETWORK PEOPLE'S business, (collectively, the "NETWORK PEOPLE Covered Claims"). NETWORK PEOPLE. agrees to reimburse COMPANY for the expense and cost of handling such claims including, without limitation, legal fees.

6.3. Notice Procedure. NETWORK PEOPLE will provide COMPANY with prompt written notice of each COMPANY Covered Claim of which NETWORK PEOPLE becomes aware, and, at NETWORK PEOPLE'S sole option, NETWORK PEOPLE may elect to participate in the defense and settlement of any COMPANY Covered Claim with COMPANYS' Consent, provided that such participation shall not relieve COMPANY of any of its obligations under this Section 6. COMPANY shall have the right to control the defense of any COMPANY Covered Claim. COMPANY will provide NETWORK PEOPLE with prompt written notice of each NETWORK PEOPLE Covered Claim of which COMPANY becomes aware, and at COMPANY'S sole option, COMPANY may elect to participate in the defense and settlement of NETWORK PEOPLE Covered Claim, provided that such participation shall not relieve NETWORK PEOPLE of any of its obligations under this Section 6. NETWORK PEOPLE shall control the defense of any NETWORK PEOPLE Covered Claim.

7. No poaching.

Both NETWORK PEOPLE and COMPANY agree to NOT poach employees from each other throughout the term of this agreement and any extensions. If an employee of NETWORK PEOPLE is hired directly by COMPANY as an employee or indirectly by COMPANY as a contractor under any payment arrangement, COMPANY agrees to pay NETWORK PEOPLE the equivalent of three (3) years current compensation package for that employee (including salary, bonuses, retirement, and benefits) within 15 days of the hiring of that employee to cover training and replacement costs. Conversely, if an employee of COMPANY is hired directly by NETWORK PEOPLE as an employee or indirectly by NETWORK PEOPLE as a contractor under any payment arrangement, NETWORK PEOPLE agrees to pay COMPANY the equivalent of three (3) years current compensation package for that employee (including salary, bonuses, retirement, and benefits) within 15 days of the hiring of that employee to cover training and replacement costs. Both companies, however, can make an exception to this clause if the terms of the hiring are agreed upon in writing BEFORE any conversation with the employee.

8. Cancellation/Termination.

8.1. Cancellation by COMPANY and Early Termination Fee. COMPANY must give NETWORK PEOPLE at least ninety (90) days written notice of any cancellation or termination of services. COMPANY must send an email or fax with Company letterhead to NETWORK PEOPLE fax number located at their website or to Billing@NetworkPeople.com; document must include the COMPANY name, description of services and effective cancellation date. In circumstances where COMPANY chooses to terminate the agreement early, COMPANY agrees to reimburse NETWORK PEOPLE for any and all discounts realized (as detailed in the Recurring Expense Summary section describing Discount(s)) when signing the agreement and agrees to pay 180 days (6 months) worth of the full non-discounted rate of the monthly agreement rate (calculated based on the average rate paid for services to date on the agreement) as an Early Termination Fee.

8.2. Cancellation by NETWORK PEOPLE. NETWORK PEOPLE reserves the right to terminate COMPANY for any reason. NETWORK PEOPLE will provide the COMPANY with ninety (90) days advanced written notice of termination of contract for cause and will allow the COMPANY ninety (90) days to cure any breach. NETWORK PEOPLE also reserves the right to withhold any refunds to COMPANY, NETWORK PEOPLE must give COMPANY at least ninety (90) days advanced written notice of cancellation.

8.3. Bankruptcy. NETWORK PEOPLE may terminate this Agreement upon written notice to COMPANY if COMPANY becomes the subject of a petition in bankruptcy or any proceeding relating to insolvency, receivership, or liquidation for the benefit of creditors, if such petition or proceeding is not dismissed within 60 days of filing.

8.4. For Other Cause. Except as otherwise stated, either party may terminate this Agreement if the other party breaches any material term or condition of this Agreement and fails to cure such breach within ninety (90) days after receipt of written notice of the same.

8.5. Effect of Cancellation or Termination. Upon expiration or termination of this Agreement: (a) NETWORK PEOPLE will cease providing the Services; (b) all of COMPANY payment obligations under this Agreement, including but not limited to monthly Service Fees through the end of the Term will become due in full immediately; and (c) within ninety (90) days, NETWORK PEOPLE will remove all NETWORK PEOPLE Equipment and any other owned property from COMPANYS premises. If COMPANY does not allow NETWORK PEOPLE access to its Equipment within the ninety (90) day period, NETWORK PEOPLE, at its option and at COMPANY expense, may use whatever means necessary to remove the Equipment. NETWORK PEOPLE will return all COMPANY Equipment within the ninety (90) day period. In addition, NETWORK PEOPLE reserves the right to hold any COMPANY Equipment until it has received payment in full.

9. Survival.

The Parties' respective representations, warranties, and covenants, together with obligations of indemnification, confidentiality and limitations on liability will survive the expiration, termination or rescission of this agreement and continue in full force and effect.

10. Service Disclaimer.

COMPANY grants NETWORK PEOPLE authorization to view any files within the regular routine of the repair or system improvement. COMPANY also authorizes NETWORK PEOPLE to reasonably delete, change, and/or rewrite any necessary information to complete the system repair or improvement that is consistent with the standards and practices in the industry.

11. Confidentiality.

NETWORK PEOPLE and its agents will not use or disclose COMPANY information, except as necessary to or consistent with providing the contracted services and will protect against unauthorized use.

12. Disputes.

In the event of any dispute between the parties, the parties agree to attempt to resolve the dispute in good-faith through a face-to-face meeting. In the event of any dispute which the parties cannot resolve after face-to-face good-faith discussions, the parties agree to participate in non-binding mediation within fourteen (14) days after demand for mediation by either party, prior to filing any litigation. The non-requesting party will choose the mediator. The costs of the mediation will be shared equally by the parties. If either party files any litigation prior to participating in mediation, then that party will pay all costs incurred, including legal fees, in having the matter dismissed or stayed pending mediation. Parties agree that the forum for any arbitration, mediation, or litigation shall be the Circuit Court of Pinellas County.

13. Award of Expenses.

In the event that either party must take any action to enforce any term of this Agreement, including payment, each party agrees to pay their own attorneys' fees and all their own costs, including but not limited to expert witness fees, court and process costs.

14. Provision for Other Agencies. Piggybacking Clause.

Unless otherwise stipulated, NETWORK PEOPLE agrees to make available to all "Eligible Users" the prices submitted in accordance with the terms and conditions of the contract resulting from this solicitation. Eligible Users means all State of Florida government agencies, the legislature and judicial branches, and political subdivisions (counties, local district school boards, community colleges, municipalities, or other public agencies or authorities), which may desire to purchase under the terms and conditions of the resulting contract.

15. General.

This Agreement and the rights, duties, obligations and liabilities of the parties under this Agreement and all amendments, modifications, authorizations or supplements to this Agreement shall be determined in accordance with the applicable provisions of the laws of the United States of America and of the State of Florida, as applicable to contracts made and to be performed entirely within that state, without reference to its doctrines or principles of conflicts of laws. Any action or proceeding arising out of or relating to this Agreement and the agreements, instruments, documents and other papers contemplated hereby shall be brought in the United States District Court for the District of Florida, or any state courts for the State of Florida situated in Pinellas County. The parties hereby consent to and agree to submit to the exclusive jurisdiction of such courts and waive and agree not to assert, in any dispute, to the fullest extent permitted by applicable law, any claim that (i) such party is not personally subject to the jurisdiction of such courts, (ii) such party and such party's property is immune from any legal process issued by such courts, or (iii) any litigation commenced in such courts is brought in an inconvenient forum.

16. Acts of God.

NETWORK PEOPLE is not responsible for failure to render services due to circumstances beyond its control including, but not limited to, acts of God.

Service Descriptions

Additional DC Server Support

Daily monitoring and management of server and repair when needed. This is custom service and support for servers that ONLY function as Active Directory Domain Controller (a server dedicated to security authentication requests within a Windows Server Domain). Network People engineers perform daily health checks before business hours. This includes runtime and stability, backed, and critical errors. Then engineers verify additional health and security checks through monitoring and management of antivirus, anti-malware, system checks, alerts, hard drive maintenance, specific scripted repairs of known issues, ticket creation and closure. If an issue is detected, a ticket is created notifying client and an engineer dispatched to perform the necessary service according to the SLA to restore normal functionality. If ticket requires repair to be done onsite, the engineer will go onsite.

Advanced Security Monitoring

Proactive, persistent threat protection for your network that identifies your vulnerabilities and allows earlier detection of ransomware activity. This advanced security detection delivers: Vulnerability scanning, alert review and recommendations, remediation direction, detection and review of indications of compromise through ongoing scanning and monitoring for vulnerabilities. Network People engineers use state-of-the-art security tools that detect indications of compromise (IOC) on computers or servers in the network. When new or greater risks are identified, Network People alerts you. This security monitoring: • Highlights external and internal vulnerabilities to tighten your defenses • Enables earlier detection of potential ransomware incidents • Exposes attackers who abuse legitimate Windows applications and processes to bypass other security systems and establish persistence • Reviews incident reports that combine automated intelligence with human expertise to understand the scope and severity of potential threats • Prevents hackers from dwelling in your protected environments with step-by-step guidelines to harden your security and reduce future risk (Security + Monitoring + Compliance + Management + Proactive Maintenance + Accountability)

Azure Server Standard License and AD Server Support

Custom service and support for Azure AD services which gives users seamless access to all applications to maintain productivity. Network People engineers perform additions and subtractions of Microsoft Licenses of all kinds on the Azure server and manage the users access, data, security, and overall licensing. Engineers also enable the connection of workstations and laptops to the Domain Controller of the Azure AD. If an issue is detected, a ticket is created notifying

client and an engineer dispatched to perform the necessary service according to the SLA to restore normal functionality. If ticket requires repair to be done onsite, the engineer will go onsite. (Monitoring + Management + Helpdesk + Proactive Maintenance + Security + Compliance)

Azure Cloud Server Support

Daily monitoring and management of cloud server and repair when needed to keep your network and team up and running. A private off premise cloud server hosted at a Microsoft data center used for storage, data bases, permissions access control, and file and print. Creates a highly redundant solution with flexibility for growth and scale. (Management + Security + Monitoring + Proactive Maintenance + Helpdesk)

Azure Usage

Management and provision of Cloud hosting services. Monthly variable rate for cloud hosting expenses in the Azure data center for the following services: Bandwidth utilization, number of servers, total storage, and resources.(Management)

Backup Server Alto 1TB

This disaster recovery tool offers comprehensive full server protection and minimizes network downtime. It prevents data loss, ensures quick full system restores, and easy recovery of individual files. Redundancy (full image back-ups of your server) in two data centers outside the state of Florida. Allows us to do image backup as often every 15 minutes. NPI engineers confirm backup was tested, successful, and complete every morning before business and proactively fixing any problem that are detected. (Disaster Recovery + Business Continuity + Security+ Compliance + Monitoring + Proactive Maintenance + Management + Helpdesk)

Cloud Backup & Archiving for Email & Office 365

This backup system for MS 365 protects from the threat of ransomware, data loss, or sabotage. This automated cloud-based backup and archiving system protects all OneDrive and Microsoft 365 data including (Word, Excel, Outlook, PowerPoint, Publisher, Access, OneNote, OneDrive, Teams, and many other applications in the MS 365 stack as well as personal documents and data stored in the OneDrive system). (Disaster Recovery + Proactive Maintenance + Security + Compliance + Disaster Recovery + Business Continuity + Helpdesk)

Vulnerability Scanning

This tool vulnerability assessment & management system to help safeguard their business critical systems and data. Built by MSP industry pioneers to solve the cybersecurity problems MSPs face, it leverages a collaborative model of product development that integrates MSP insights. Scan network gear such as routers; switches; access points; firewalls; end-user devices, such as laptops and desktops; printers; and servers and virtual machines.

Customized Client Dashboard

Provides a real-time digital report on how your network, resources, and IT management are delivering value to your organization. This tool pulls information from multiple systems that monitor and protect your network as well as gathers data to help the business leader make decisions about technology, resources, and budgeting. It compiles it all into one easy to use and understand set of graphs and tables on one dashboard. (Strategy + Accountability + Monitoring)

Cyber Security Training

Your best assets are also your greatest security risk. Human error is the main cause of data and security breaches. At Network People, we've seen this firsthand. That's why we are now providing ongoing security training for your employees that is tailored to the security threats and risks they face daily. This includes everything from email phishing scams to what to do if they think there's been a security breach.

Security Awareness Training. It should be fun! The platform trains your employees with short, memorable security awareness stories. Our security awareness training content is fun, memorable, and will have your employees begging you to watch the next episode!

Choose from a variety of fresh new training content, episodes, security awareness downloads, phishing simulations, and more.

Reporting. Our executive summary reports highlight your program at a glance, and detailed reports help you zoom in for compliance audits and more granular views that Compliance Auditors Will Love!

Get a snapshot all of your evidence and online training records in seconds. Reporting will demonstrate compliance of your entire security awareness training program.

Datto: Siris Backup

A backup server with redundancy in two locations outside of Florida to keep your business running even in the middle of disasters such as ransomware, malware, hurricanes, network downtime, and human errors. It includes verified backups as often as every five minutes, data restoration, ransomware protection, and instant virtualization (if the server goes down, we'll take the backup and make that the server within minutes so everyone gets back to work). All backed by Datto's private cloud. NPI engineers confirm backup was tested, successful, and complete every morning before business and proactively fixing any problem that are detected. Compliance + Monitoring + Proactive Maintenance + Management + Helpdesk)

Email Security Filtering for Business

Email Fraud Defense protects your employees, customers, and business partners from cyber criminals who spoof trusted email domains. It makes email authentication easy and reliable so you can stop email fraud before it reaches the inbox. It blocks socially engineered attacks such as business email compromise and consumer phishing and automatically adjusts to new vectors of attacks created by criminals. Simplify email authentication without blocking legitimate email. Provides: email antivirus, spam filtering, reporting, content filtering, outbound filtering, imposter email protection, and data loss prevention. (Monitoring + Security + Business Continuity + Proactive Maintenance + Management + Compliance + Helpdesk)

Email Security Filtering with Encryption

Email Fraud Defense protects your employees, customers, and business partners from cyber criminals who spoof trusted email domains. It makes email authentication easy and reliable, so you can stop email fraud before it reaches the inbox. It blocks socially engineered attacks such as business email compromise and consumer phishing and automatically adjusts to new vectors of attacks created by criminals. Simplify email authentication without blocking legitimate email. Provides: email antivirus, spam filtering, reporting, content filtering, outbound filtering, imposter email protection, and data loss prevention. Also includes Email encryption, attachment defense (sandboxing), and social media account protection. (Monitoring + Security + Business Continuity + Proactive Maintenance + Management + Compliance + Helpdesk)

Email Security Filtering with Encryption and Archiving

Email Fraud Defense protects your employees, customers, and business partners from cyber criminals who spoof trusted email domains. It makes email authentication easy and reliable, so you can stop email fraud before it reaches the inbox. It blocks socially engineered attacks such as business email compromise and consumer phishing and automatically adjusts to new vectors of attacks created by criminals. Simplify email authentication without blocking legitimate email. Provides: email antivirus, spam filtering, reporting, content filtering, outbound filtering, imposter email protection, and data loss prevention. Also includes Email encryption, Archiving, attachment defense (sandboxing), and social media account protection. (Monitoring + Security + Business Continuity + Proactive Maintenance + Management + Compliance + Helpdesk)

Gateway Security For Firewall

Daily firewall management for prevention and detection against threat actors/hackers. Network People engineers manage the firewall and daily review the best settings and configurations and latest software (Firmware) to tune the firewall in order to provide the best prevention and detection against threat actors/hackers. (Security + Compliance + Monitoring + Proactive Maintenance + Management)

Hardware as a Service Support

Support for the management of hardware and software (inventory, purchase, replacement, and vendor support) Basic support for Hardware as a Service to manage inventory, asset allocation, sourcing of product, warranty, and vendor issues. (Management + Compliance + Proactive Maintenance + Accounting)

H365 Email MDR

Managed Detection and Response (MDR) for Microsoft 365 product.

Service Description:

1. We possess advanced technology and specialized knowledge across various IT domains, including cybersecurity, enabling us to provide reliable solutions, proactive maintenance, and effective troubleshooting
2. We offer 24/7 monitoring of your IT systems, ensuring issues are identified and addressed promptly. This proactive approach minimizes downtime and disruptions and reduces the risk of breaches and data loss, which are crucial for businesses like yours. Additionally: You get access to a team of professionals at a fraction of the cost of building out your own security team, enabling you to concentrate on your core business.

How we protect against BEC:

1. We have a powerful managed detection and response (MDR) solution included in our security services that secures your cloud identities and applications from BEC scams.
2. By detecting and responding to suspicious user activity, permission changes, and anomalous access behavior, and backed by a 24/7 SOC team, our solution empowers us to fight back against attackers on your behalf, with no gaps or lags in coverage during the peak seasons, off hours, or holidays.

About Business Email Compromise (BEC):

Since BEC attacks are generally human-centric, the methods of protection and prevention must also be human-centric.

By partnering with us, you get access to a team of dedicated security experts who are working for you day and night to catch and contain BEC attacks.

Managed Active-IT User

Unlimited management and helpdesk support for a user (Onsite & Remote). During normal business hours Network People technician repairs desktop/laptop, verifies monitoring and management of desktop(s) is done correctly and successfully. This includes antivirus, anti-malware, system checks, alerts, hard drive maintenance, specific scripted repairs of known issues, ticket creation and closure. If Network People detects an issue with any of the above, a ticket is created notifying client and a technician is dispatched to perform the necessary service according to the SLA to restore normal functionality. If ticket requires repair to be done onsite, the technician will go onsite. All the following repairs will be performed under the "unlimited" coverage. *Replace or repair hardware (actual hardware part must be purchased by client) *Conference with vendor to get warranty repair that client deserves *Restore deleted files (requires backup server) *Provide training, advice, troubleshooting, and general user support (Management + Helpdesk + Security + Compliance + Proactive Maintenance + Disaster Recovery + Business Continuity)

Managed Active-IT Chromebook User

Remote services covered. Hardware/troubleshooting/repair is OOSA.

Managed Active-IT Remote Only User

Unlimited management and helpdesk support for a user (Remote Only). During normal business hours Network People technician repairs desktop/laptop, verifies monitoring and management of desktop(s) is done correctly and successfully. This includes antivirus, anti-malware, system checks, alerts, hard drive maintenance, specific scripted repairs of known issues, ticket creation and closure. If Network People detects an issue with any of the above, a ticket is created notifying client and a technician is dispatched to perform the necessary service according to the SLA to restore normal functionality. If ticket requires repair to be done onsite, the technician will go onsite. All the following repairs will be performed under the "unlimited" coverage. *Replace or repair hardware (actual hardware part must be purchased by client) *Conference with vendor to get warranty repair that client deserves *Restore deleted files (requires backup server) *Provide training, advice, troubleshooting, and general user support (Management + Helpdesk + Security + Compliance + Proactive Maintenance + Disaster Recovery + Business Continuity)

Managed Cloud Backup for Workstations

Tool that provides daily backup for workstations and is monitored for success. Full image backup of computer's hard drive up to 1 TB into offsite data center replicated in two locations outside the state of Florida. Backups occur once per day. It provides: a full image cloud backup, screenshot verification, restore and virtualization of the entire PC, including files and data stored locally. (Disaster Recovery + Monitoring + Proactive Maintenance + Security + Helpdesk)

MAC Time Machine Backup

Monitoring of the backup for a MAC. Alerts when the backup has not been successful for 7 days. Works with our Remote Management Tool (Mac). *This service requires external hard drive or NAS device.

Managed Endpoint SOC Protection

Advanced endpoint detection and protection combined with SOC-based response and remediation services. On-demand security operations. Always-on threat coverage. Next-gen threat detection and remediation. *Protection: Deliver complete endpoint protection and monitoring. Out static artificial intelligence (AI) prevents attacks before they start by monitoring and analyzing client IT environments. *Threat detection: Behavioral AI constantly monitors and maps each running process for incongruous behaviors and recognizes many thousands of virus and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors by quickly identifying and diagnosing corrupt source processes and system settings. *Response and remediation: When malicious behavior is detected, Managed Endpoint will activate remediation steps including scrubbing the system of any remnant of an attack, such as malicious processes or registry keys, and performing system rollback, if required, to restore system and data access. *Managed detection and response (MDR): Implement advanced operations without the need for in-house security expertise. *Next-gen endpoint security: Provides unique malware detection and remediation technology. This solution incorporates innovative prevention technology, providing visibility into the root causes and origins of the threat, reversing the malicious operations of ransomware and remediating them at an agile speed, when needed. (Security + Monitoring + Compliance + Management + Proactive Maintenance + Accountability)

Network Map

Professional Network Mapping tool that auto-senses devices on the network that have an IP address and makes a visual diagram of those devices for ease of inventory and security. Also helps with securing the network when rogue devices are autosensed—such devices can be removed from the network to prevent unauthorized or malicious access. (Management + Monitoring + Proactive Maintenance + Security + Accountability + Compliance)

Parallels Monitoring & Support (MAC)

Support for parallels running on a MAC. Technical support to troubleshoot, configure, and train user for help with parallel software running on top of the MAC. (Management + Proactive Maintenance + Helpdesk)

Privileged Access Management

A system to stop hackers from remotely escalating permissions on the desktops and installing malicious code or ransomware or pivoting to another computer or server on the network. It allows users to escalate permissions to install applications or printers but do so in a secure approach that doesn't leave the system vulnerable to outside breaches. (Security + Monitoring + Compliance + Management + Helpdesk)

Remote Management Tool

A monitoring and management tool that saves time and money by giving NP engineers the ability to securely remote into the machine with the user's permission and diagnose and solve the problem or provide user training if needed. IT allows Network People engineers to have a full team of resources, knowledge, and tools to identify and solve problems. This includes providing information so in depth about every computer and server on the network that our engineers have real time information about the firmware of the bios, the version of the operating system, all the software installed on system and their versions, technical information about setup of the computer, all the drivers, data, and much more. In addition, Network People has programmed custom scripts to identify issues automatically and resolve those issues without any user involvement. This saves you time and money. These custom scripts are continuously improved by watching for problems in the hundreds of networks that we manage, which helps us to identify and proactively prevent problems on your network. (Security + Monitoring + Compliance + Management + Proactive Maintenance)

Remote Management Tool (Mac)

Actively monitors for problems on devices before they happen and prevents downtime. Remote monitoring for and remediation of issues. Keeps track of every device in your network regardless of location. Real-time visibility of your inventory. (Security + Monitoring + Management + Compliance)

Server backup – Physical server

On-premises full image and file level server backup to protect your business and keep you up and running. System schedules regular backups as often as hourly and creates differential backup sets (backups of recently changed files) for full recovery or file-based retrieval of data. Image backups can be stored on local media (SAN, backup server, tape) and in redundant locations off-premises. Backups are monitored and managed by the Network People team daily during normal business hours and tickets created automatically to have engineers repair if the backups fail. (Disaster Recovery + Management + Monitoring + Proactive Maintenance + Security + Compliance + Disaster Recovery + Business Continuity)

Server backup – Virtual server

On-premises full image and file level server backup to protect your business and keep you up and running. System schedules regular backups as often as hourly and creates differential backup sets (backups of recently changed files) for full recovery or file-based retrieval of data. Image backups can be stored on local media (SAN, backup server, tape) and in redundant locations off-premises. Backups are monitored and managed by the Network People team daily during normal business hours and tickets created automatically to have engineers repair if the backups fail. (Disaster Recovery + Management + Monitoring + Proactive Maintenance + Security + Compliance + Disaster Recovery + Business Continuity)

Server Room (NOC) Management

Maintain, configure, and support equipment in server room. Equipment includes rack, uninterruptable power supply (UPS), switch, firewall. *Labor to replace or repair hardware (actual hardware part must be purchased by client)

*Conference with vendor to get warranty repair that client deserves *Fix normal, high, and critical issues (Disaster Recovery + Management + Monitoring + Proactive Maintenance + Security + Compliance + Disaster Recovery + Business Continuity + Helpdesk)

Unified Alerting, Documentation Management

Alerts to system compliance issues and resolves them which prevents downtime. Network People combines a powerful set of tools into a unified control panel to provide best in class alerting, documentation, inventory, and change management. Information about hardware and software is instantly gathered and documented. If the information shows that a system is out of compliance an alert is created. It also proactively identifies and resolves changes through these automated alerts and prevents downtime. Engineers can quickly evaluate the system using automated security, compliance, and network configuration alerts. The impact: The business can worry less because misconfigurations or security compliance issues are identified and alerted upon. Troubleshooting is easier because the history of the machine is recorded which makes it possible for engineers to go back in time to figure out what change caused the issue. (Disaster Recovery + Management + Monitoring + Proactive Maintenance + Security + Compliance)

Virtual Server Support

Daily monitoring and management of server and repair when needed to keep your network and team up and running. Network People engineers perform daily health checks before business hours. This includes runtime and stability, backed, critical errors. Then engineers verify additional health and security checks through monitoring and management of antivirus, anti-malware, system checks, alerts, hard drive maintenance, specific scripted repairs of known issues, ticket creation and closure. If an issue is detected, a ticket is created notifying client and an engineer is dispatched to perform the necessary service according to the SLA to restore normal functionality. If ticket requires repair to be done onsite, the engineer will go onsite. All the following repairs will be performed under the "unlimited" coverage of the server at no extra charge. Examples of such repairs include: *Fix Active Directory (AD) and Group Policy Objects (GPO) issues *Replace or repair hardware (actual hardware part must be purchased by client) *Conference with vendor to get warranty repair that client deserves *Restore data on hard drive or restore entire server (requires backup server) *Provide training, advice, troubleshooting, and general user support (Management + Helpdesk + Security + Compliance + Proactive Maintenance + Disaster Recovery + Business Continuity)

2FA Protection and Management

Prevents unauthorized access to email, Windows Domain, and Cloud accounts. This is designed to prevent unauthorized access to your network by requiring both a password and something you know (the second factor) to have access to the account. For example, a security code is sent to your cell phone. This system manages two-factor authentication (2FA, MFA) devices and improve security for remote desktop connections. This can be implemented for most third-party web facing applications including connecting to the corporate network remotely. Network People can manage the users to maintain high security and compliance, so the tool isn't turned off by users, exposing the network to risk. (Security + Management + Compliance + Helpdesk)

3rd Party Application Updates

Maintains proper updates to network computers and servers to protect from hackers. Statistics show that as high as 97% of malicious code would be prevented from impacting computers and servers if they were properly and regularly updated. This tool and service allows your network computers and servers to maintain the proper updates both in Microsoft operating systems as well as third party applications. (Security + Compliance + Management + Proactive Maintenance)

EXHIBIT A



13075 US Highway 19 N
Clearwater, FL 33764
www.NetworkPeople.com
(727) 446-4564

User & Site Support

Description	Recurring	Qty	Ext. Recurring
Managed Active-IT User Unlimited management and helpdesk support for a user (Onsite & Remote).	\$78.00	85	\$6,630.00
Cyber Security Training End user cyber security training with monthly updates and customer portal to provide record for compliance.	\$5.40	85	\$459.00
Virtual Server Support Full monitoring and management of a virtual server.	\$240.00	5	\$1,200.00
Managed Security- 4 hrs per quarter & monitoring Proactive, persistent threat protection for your network that identifies your vulnerabilities and allows earlier detection of ransomware activity. This advanced security detection delivers: Vulnerability scanning, alert review and recommendations, remediation direction, detection and review of indications of compromise through ongoing scanning and monitoring for vulnerabilities. Network People engineers use state-of-the-art security tools that detect indications of compromise (IOC) on computers or servers in the network.	\$1,250.00	1	\$1,250.00
Managed Environment Package	\$744.00	1	\$744.00
Customized Client Dashboard Provides a real-time digital report on the management of your IT.		1	
Gateway Security for Firewall Network People engineers manage the firewall and daily review the best settings and configurations and latest software (Firmware) to tune the firewall.		2	
** Requires new hardware /sonicwalls to be purchased (formal quote to follow).			
Server Room (NOC) Management Maintain, configure, and support equipment in server room.		4	
For detailed descriptions see NetworkPeople.com/Service-Descriptions			

Monthly Subtotal: \$10,283.00

Device Tools- PC & Server

Description	Recurring	Qty	Ext. Recurring
Remote Management & Updating Tool Remote Management & Updating Tool	\$3.00	75	\$225.00
Breach Detection MDR Real time "active threat" detection and response.	\$7.20	75	\$540.00

Device Tools- PC & Server

Description	Recurring	Qty	Ext. Recurring
Advanced Security Monitoring Proactive, persistent threat protection.	\$6.00	75	\$450.00
Privileged Access Management A system to stop hackers from remotely escalating permissions.	\$3.60	75	\$270.00
Vulnerability Scanning Assists in meeting compliance requirements by detecting deficiencies and providing comprehensive information to resolve issues.	\$1.20	75	\$90.00
For detailed descriptions see NetworkPeople.com/Service-Descriptions			

Monthly Subtotal: \$1,575.00

Licenses

Description	Recurring	Qty	Ext. Recurring
365 Email MDR Managed Detection and Response (MDR) for Microsoft 365 product.	\$2.50	113	\$282.50
Microsoft 365 Apps for Business Includes fully installed Office applications across multiple devices plus online file storage and sharing.	\$8.30	1	\$8.30
Microsoft Office 365 E3 (Users 300+) Includes fully installed Office applications across multiple devices, email hosting, HD video conferencing, and features to support compliance	\$23.00	85	\$1,955.00
Microsoft Exchange Online (Plan 1) Hosted Email	\$4.00	24	\$96.00
Microsoft Project Plan 1 Microsoft Project Plan 1 enables users to start quickly and manage projects easily via a web browser.	\$10.00	1	\$10.00
Azure Active Directory Premium P1	\$6.00	1	\$6.00

Monthly Subtotal: \$2,357.80

Cloud Services

Description	Recurring	Qty	Ext. Recurring
Phone Service (billed direct from phone company - \$) Full image managed backup of computer up to 1 TB.	\$0.00	1	\$0.00
Print Management (Xerox printers- approximate cost) *Cost varies based on print usage	\$700.00	1	\$700.00

Cloud Services

Description	Recurring	Qty	Ext. Recurring
Backup Server Siris S4P6 A backup server with offsite redundancy in two data centers outside of Florida. With onsite virtualizations, keep your business running even in the middle of disasters. For detailed descriptions see NetworkPeople.com/Service-Descriptions	\$1,279.00	1	\$1,279.00

Monthly Subtotal: \$1,979.00

Monthly Expenses Summary

Description	Amount
User & Site Support	\$10,283.00
Device Tools- PC & Server	\$1,575.00
Licenses	\$2,357.80
Cloud Services	\$1,979.00

Monthly Total: \$16,194.80

Payment Options

Description	Payments	Interval	Amount
Term Options			
5 Year agreement	60	Monthly	\$16,194.80

Summary of Selected Payment Options

Description	Amount
Term Options: 5 Year agreement	
Selected Recurring Payment	\$16,194.80

Network People, LLC

Signature:

Nate Freeman

Name:

Nate Freeman

Title:

President

Date:

02/12/2024

City of Madeira Beach

Signature:

Re 7 8

Name:

Robin Gomez

Date:

3-19-24