SCHEDULE FOR MANAGED SERVICES

This Schedule for Managed Services ("Schedule") forms part of, and is governed by the Online Agreements (as defined in the Master Service Agreement) referenced in the applicable Order between the client identified in the applicable Order ("Client") and Optimized Computer Solutions, Inc. d/b/a OCSIT ("Provider"), each of which may be referred to individually as a "Party" and collectively as the "Parties."

By signing an Order that references the Online Agreements or by continuing to receive or use any Services covered by this Schedule, Client agrees to be bound by the terms of this Schedule.

Provider's Obligations
Provider will provide the Services listed in the Quote accompanying this Schedule to the standards listed in this Schedule. Services available from Provider but not otherwise listed in the Quote are considered out of scope until such time as Client elects to purchase such services.

Client's Obligations
Provider aims to offer well rounded solutions to provide for a robust technology infrastructure. Provider's offerings all serve a purpose in achieving the end result we desire for Client. Although it is ultimately Client's decision which services Client selects (as enumerated in the Quote), we encourage Client to consider all applicable services listed in this Schedule. Know that by declining any of the services we offer, Client is hereby acknowledging and accepting the risk associated with an incomplete infrastructure. Client agrees and understands that if there is a system failure or data loss that may have been prevented by one or more the recommended but declined services, Provider will not held responsible for any data loss or network failures.

Client further acknowledges that some security breaches involve attacks on computer systems and data. For example, there are viruses and other malware that: (i) delete or destroy data (sometimes individual files, but sometimes even an entire disk by corrupting a master boot record or other key element); (ii) modify files (such as parasitic malware that attaches itself to a file and modifies the file to enable its own execution and/or propagation); (iii) encrypt files on systems (such as ransomware that uses asymmetric encryption); and (iv) seek to exfiltrate data for the attackers' personal gain (such as selling information on the "black market"). In addition, there are certain attacks that prey on humans being trustworthy, such as phishing attacks and social engineering schemes. Certain Services offered by Provider are intended to reduce the probability of these attacks occurring on a Client system. Provider cannot guarantee that the Services will prevent all such occurrences of attacks, especially human-based incidents. Moreover, while Provider may offer recommendations to enhance the overall security of Client's systems, data, and network, Provider is not responsible for creating Client's security policies and will merely implement the policies as provided by Client (including HIPAA- and PCI-related settings). Provider will use commercially reasonable efforts in the event of a data attack to reverse the effects of the attack if Client has subscribed to one of our services offering this support; however, Client is ultimately responsible for the business continuity and operation of its computer systems and ensuring that data is properly backed up and able to be restored. Provider strongly suggests Client obtain adequate cyber liability insurance from a reputable carrier and that Client's policies and procedures and aligned with the requirements of the elected cyber liability insurance policy.

Client is responsible for paying all fees for Services when due, responding to Provider's requests within a reasonable amount of time, reporting to Provider any additions or removals to the Services within a reasonable time to allow Provider to schedule its portion related to any such addition or removal, and complying with any other reasonable request of Provider.

(1) Essential IT Services

Provider's Essential IT Services package is the foundational offering for managed services and includes the essential items every company needs to support its IT environment. This package includes the following components:

Workstation and Laptop Management
Provider will conduct preventative maintenance activities for in-scope devices, including:

1. Patch Management and installation of critical OS patches
2. Asset Management and Reporting
3. Executive Reports
4. Remote Access Software
5. Client Access to remote access software
6. Basic Monitoring and Reporting
7. Basic Application Help Desk Support
8. Basic remote support of printers, scanners, and other peripheral devices
9. Remote remediation

Client's software licenses are not included in managed services.

Server Support
Provider will remotely monitor in-scope servers to detect and report problems, mitigate against data loss, mitigate downtime, and avoid repair problems. Services Include:

1. Microsoft critical updates
2. Asset Management and Reporting
3. Executive Reports
4. Basic monitoring and alerting including CPU, Disk Space, Memory, and Network Utilization
5. Endpoint Security
6. Remote Access Software
7. Remote Remediation
8. Onsite Remediation (when applicable and necessary)
9. Exchange Server Monitoring (if applicable and in-scope)
10. Database Server Monitoring (if applicable and in-scope)

Next-Generation Antivirus
Provider will supply antivirus software to in-scope devices that includes monitoring and management.

Basic Network Support
Provider will provide support services for Client's owned firewalls and switches which may include:

1. Quarterly backups and firmware updates
2. Basic configuration

(2) Helpdesk Services
Provider's helpdesk services offering provides remote support to respond timely to technical problems reported by Client's users, including issues with computers, network connections, software applications, and other technology resources. Helpdesk services are tracked using Provider's ticketing system, which allows for efficient handling of problems along with reporting capabilities and escalation of complex issues to higher-level technical teams and coordinating with others when necessary. Provider shall also provide best-effort support for non-standard software applications and systems. Provider recommends maintaining a support contract with third-party software vendors. Helpdesk services are provided during the hours of 7:30 a.m. to 5 p.m. Eastern Time on normal business days (holidays excluded).

(3) Advanced Cybersecurity
Provider's advanced cybersecurity offering is recommended for all companies with information to protect and systems that need to remain online to serve business needs. This offering includes the following components:

Enhanced End Point Security
Provider will supply end point security services to in-scope devices and accounts that includes (as applicable):

1. Enhanced endpoint monitoring and reporting via a Security Operations Center (SOC)
2. Monitored alerts for suspicious activities
3. Web-based security training modules
4. Security tips, tricks, and training
5. Simulated phishing tests to Client's own primary email domain
6. Dark-Web Monitoring
7. External vulnerability scanning on a recurring basis (as often as weekly, but not less than monthly)

Microsoft 365 Email Protection
Provider will supply managed detection and response threat analysts to monitor and respond in real-time to critical security events within Client's Microsoft 365 environment, including unauthorized communications to proprietary communications, data loss via unapproved external forwarding, and email tampering to commit financial fraud.

(4) Add-On Services
Provider understands its customers' IT environments have unique needs and may require additional services. Provider therefore offers the following add-on services, which may be included in an Order.

VoIP
Provider will provide basic services to support Client's existing phone server.

1. Configuring phone extensions
    a. Adding /removing users
    b. Password changes
2. General user support
3. Configuring IVR functionality
4. Configuring call queues
5. Backup of phone server configuration
6. Phone server maintenance and updates

Client agrees to maintain an active support contract for their phone environment.

HIPAA as a Service

1. Assist with annual HIPAA Risk Assessment
2. Provide annual workplan to address results from HIPAA Risk Assessment.
3. Provide access to all services on the hipaasecurenow.com website.
4. HIPAA Secure Now services can be reviewed at http://www.hipaasecurenow.com/index.php/service

SaaS Backup

Provider will provide SaaS backup protection for one Microsoft 365 or Google Workspace account per full time employee. The retention period and other variables can be customized based on Client's specific requirements.

IaaS

Provider will grant Client access to an Infrastructure as a Service (IaaS) environment over which Provider is a reseller. IaaS services may include:

1. Server resources (virtual)
2. Firewall resources (virtual)
3. Microsoft Operation Systems
4. Microsoft Office Suite
5. Adobe Acrobat Reader
6. Client provided software

Mobile Device Management

Provider will provide support services for Client owned iPads, which may include:

1. Automated setup of device
2. Application updates
3. Patch Management and installation

Basic Monitoring and Reporting Software licenses are not included for maintenance services.

Third Party Two Factor Authentication Management

Provider will supply services to support Client's requirement of Two Factor Authentication (2FA) with Client's compatible applications.

Additional Services and Equipment

Anything not included as part of a managed services package shall be deemed additional services or equipment. Additional services and equipment may be ordered through a Schedule for Project Services at the agreed Fees for the work and equipment. Additional services and equipment may include any of the following:

1. Project Services. examples of project services include without limitation:
    a. Installing new servers
    b. Installing or configuring new applications
    c. New location builds and installations
    d. Disaster recovery planning and testing
    e. Setting up new workstations or laptops
    f. Relocating workstations or other hardware
    g. Projects requiring four or more hours of time.
2. After-hours work. Any onsite or remote work conducted after 5 p.m. Eastern Time, on weekends, or on Provider Observed Holidays may incur an additional hourly surcharge (depending on service level).
3. Travel time. If travel to the Client's site is required or requested by Client, Client is responsible for travel costs to and from the Client's location.
4. Hardware and software.
5. 3rd-party support costs, including application, service, or device support.
6. Training. Instruction related to using a software program or how to configure an application to perform specific tasks.
7. Restore. Services required due to changes or software installations not performed by Provider or disabling the Provider's management or security software.

Technology Vendor Management

Provider will manage communications with technology vendors as agreed between the Parties.

Managed Backup and Disaster Recovery

Provider may provide backup and disaster recovery services that are customized for Client's specific regulatory and business needs. Depending on those needs, this service may require a separate Schedule to detail the offering based on Client's specificity.

Third Party HaaS Hosting

Provider may provide third party HaaS access. Resources provided can include:

1. CPU / RAM
2. Disk Storge

3. Network Connectivity
4. Internet Bandwidth
5. Backup Services
6. Backup Disk Storage
7. Firewall
8. Public IP Address
9. Microsoft Remote Desktop Licensing
10. Microsoft Office Licensing

Specialty Consulting

Provider may provide one or more of the following services that can include:

1. Executive leadership service also known as "Virtual CIO"
2. Configuration and/or Support for some or all the following technologies:
    a. Firewalls
    b. Network Switches
    c. Storage Area Networks (SAN)
    d. Virtualization Host Servers and Storage
    e. Breach and/or Compromise Remediation
    f. Disaster Recovery support
3. Vendor support including but not limited to:
    a. Research and vetting
    b. Meetings and phone calls (including during negotiations and contract discussions)

(5) Managed Service Exclusions

For the avoidance of doubt, the following list of items are excluded from managed services packages and must be procured separately, if Provider agrees to provide such items.

1. Any net new installations, additions, or major changes of covered devices.
2. Parts, equipment, or software not covered by vendor/manufacturer warranty or support.
3. The cost of any parts, equipment, upgrades, consumables, or shipping charges of any kind. Provider can help Client procure these products at preferred pricing.
4. The cost of any software, licensing, or software renewal or upgrade fees of any kind.
5. The cost of any third-party vendor or manufacturer support or incident fees of any kind.
6. The cost to bring Client's environment up to minimum standards required for Services.
7. Restoring any file or entire device due to loss, theft, damage, corruption, or any other reason; provided, however, if Client subscribed to Provider's full suite of backup management services, Provider will initiate restorations within the capabilities of the backup management service.
8. Service and repair made necessary by the alteration or modification of any component under support other than that authorized by Provider, including alterations, software installations or modifications performed by Client's employees or anyone other than Provider.
9. Security services such as forensic review or other customary services provided after detection of a security breach.
10. Maintenance of software packages, whether acquired from Provider or any other source unless otherwise specified.
11. Programming (including modification of software code), program (software) maintenance, or changes to software configurations, unless otherwise specified.
12. Training Services (other than Cyber Security Awareness Training)
13. Certifying or otherwise warrantying compliance with any security-related standards related to Client systems and environment.
14. Problems that arise from the action or inaction of Client that are contrary to Provider's reasonable recommendations or in conflict with Client's obligations under this Agreement.