Service Schedule

This WIN IT Services, LLC Service Schedule ("Service Schedule") as referenced in that certain Master Services Agreement ("MSA") between WIN IT Services, LLC and/or Digicorp, LLC (collectively and individually, "Service Provider") and the Client listed in the applicable SOW ("Client" or "Customer"). This Service Schedule further describes and defines what services Service Provider may provide to Client pursuant to an SOW. Any executed SOW, this Service Schedule, and the MSA are collectively referred to as the "Agreement." In the event of conflict or inconsistency between the foregoing documents, the documents shall control in the order listed in the foregoing sentence. Any undefined capitalized terms used in this Service Schedule shall have the meanings set forth in the MSA. Service Provider may amend this Service Schedule from time-to-time.

Service Provider may provide certain managed, technical, product resale, or professional services (collectively, "Services") related to Client's information technology ("IT") environment as expressly set forth in a SOW.

Managed Services

1. Backup Management
2. Client Portal
3. Co-Management
4. Deployment
5. Documentation
6. Infrastructure as a Service (IaaS)
7. Lifecycle Management
8. Maintenance and Updates
9. Managed Procurement
10. Monitoring
11. Onsite Support
12. Password Management
13. Support and Administration
14. Support Desk
15. Reporting
16. User Management

Technical Services

1. Technical Services

Product Resale Services

1. Backup as a Service (BaaS)
2. Product Resale

Professional Services

1. Administration
2. Deployment
3. Design
4. Discovery
5. Migration
6. Project Management

Managed Services

1. **Backup Management:** The act of performing regular device, system, or application backups with the intention of protecting data ("Client Data") and minimizing productivity loss due to mistake, failure, or malicious action. This activity can include the review of backup results, backup testing, as well as restoration activities.

Service Provider may backup and retain Client Data, in the frequency, specification, and duration as set forth in the SOW. If Client Data exceeds the data storage amount set forth in the SOW, Client will be subject to additional fees and expenses at Service Provider's then-current rates.

Backup and Retention Levels			
Level	***Backups Performed***	***Backup Schedule***	***Backup Retention***
1	Annual	Last day of calendar year	Seven (7) years
	Monthly	Last day of month	Twelve (12) months
	Weekly	Each Sunday	Four (4) weeks
	Daily	Each day	Thirty (30) days
2	Annual	Last day of calendar year	Three (3) years
	Monthly	Last day of month	Twelve (12) months
	Weekly	Each Sunday	Four (4) weeks
	Daily	Each day	Thirty (30) days
3	Annual	Last day of calendar year	One (1) year
	Monthly	Last day of month	Six (6) months
	Weekly	Each Sunday	Four (4) weeks
	Daily	Each day	Thirty (30) days
4	Monthly	Last day of month	One (1) month
	Daily	Each day	Thirty (30) days

In the event of a hardware failure, human error, software malfunction, natural disaster, or computer virus ("Disaster") that makes Client Data inaccessible or unusable, Service Provider shall provide Client with its Client Data from the most recent backup. Client Data may include information that is subject to the Health Insurance Portability and Accountability Act ("HIPAA") and the Parties may be subject to the terms and conditions of a Business Associate Agreement. Except as stated in a Business Associate Agreement between the Parties, Service Provider does not warrant that Backup Services are or shall make Client compliant with "HIPAA Rules" meaning the Privacy, Security, Breach Notification, and Enforcement Rules as set forth at 45 CFR Parts 160 and 164. Client agrees that unless specifically designated as such in the SOW, Client Data shall not include electronic protected health information. The Services are only intended to cover services provided in the United States and is not intended to cover Services Provider accessing or otherwise processing personal data of any individual located outside of the United States. If Client believes that the processing of personal data of any data subject or individual located outside of the United States (a) Client will notify Service Provider prior to providing or making assessable any such personal data, and the parties will first enter into a separate agreement or amendment addressing the processing of such personal data, including

any data transfer agreement or standard contractual clauses required by applicable law and industry standards; and (b) additional charges will apply.

2. **Client Portal:** The act of providing Clients direct access to manage tickets or see relevant statistics about ticket lifecycle for Client end-users. This can include full access to all open Client tickets, dashboards that contain organization-specific statistics about ticket state, problems, time utilization, and designed workflows for things like new user request forms and user terms.

3. **Co-Management:** The act of collaborating with designated Client staff in the day-to-day delivery of SOW specified services. Designated Client staff will be granted access to Service Provider systems and best practices to enable a collaborative use of these systems and practices to deliver Client support.

4. **Deployment:** The act of provisioning new endpoints identified in an SOW for use within a Client's IT environment. This may include the unboxing, imaging, configuration, application installation, updating, and setup of a device for an end user, with the intention of minimizing user impact and downtime. This may also include user data migration to a new device.

5. **Documentation:** The act of creating, managing, and maintaining a repository of configurations, policies, and how-to guides for the purpose of minimizing the impact of issues and maintaining environmental consistency. Certain Documentation may also be made available via a self-help portal for common problems, allowing Client end users to support themselves without opening a Support Desk ticket.

6. **Infrastructure as a Service (IaaS):** IaaS is the hosting of one or many Virtual Private Server(s) (VPS) on a shared hardware platform hosted by Service Provider where Client workloads are logically isolated from each other.

7. **Lifecycle Management:** The act of proactively managing the replacement of devices or systems to maximize uptime and assist with budget management. A lifecycle management program will typically identify all designated assets in an environment, determine a business-case usable life expectancy for said devices, and proactively replace the designated devices on a predictable schedule. Typically, a replacement schedule is established and used to stage the device replacements to distribute the expense across multiple fiscal years.

8. **Maintenance and Updates:** The act of performing routine maintenance on devices, systems, or applications identified in an SOW. This includes the update of applications, server components, or firmware against devices, systems, or applications that already exist inside the IT environment. This may also include the configuration or execution of vendor-recommended maintenance tasks. Depending on the application support level, complexity, or risk, this may require the Client to engage the application vendor to ensure that maintenance tasks are executed while minimizing potential impact to the device, system, or application.

9. **Managed Procurement:** The act of quoting and procuring hardware, software, and licensing on behalf of Client utilizing the Client's existing procurement channels.

10. **Monitoring:** The act of monitoring a device or system identified in an SOW for the purposes of reporting, capacity planning, service availability, performance impact, and change validation. Monitoring provides historic trends that can be used to identify exceptions or changes within an environment as well as assist in planning for future capacity needs in addition to quantifying general availability of systems and services. Unless otherwise identified in an SOW, devices or systems will be monitored on a twenty-four hours per day, seven days per week, three hundred sixty-five days per year basis.

11. **Onsite Support**: The act of providing in-person Services at Client's physical location. Onsite Support hours shall be allocated in the SOW at the prices set forth therein. Service Provider shall designate, assign, or reassign its personnel, at its sole discretion, to provide the Onsite Support. In the event Onsite Support is requested, scheduled, and then cancelled or postponed by Client within seven (7) days of the scheduled Services, Client shall be liable to Service Provider for any Onsite Support hours not redeployed by Service Provider to another client in place of the scheduled Onsite Support as if those Onsite Support hours were provided to Client.

12. **Password Management:** The act of providing a consistent user experience, workflow, and security validation technique in the event that a user's password expires or is forgotten. This is delivered through a support desk Service Request. The intention of this practice is to return the user to work as quickly as possible while also verifying their identity to ensure that they should have access.

13. **Support and Administration:** Support and Administration are two distinct acts. While Administration is available without Support, Support is not available without Administration. Administration is the act of configuration or setup of a device, system, or application to vendor-recommended standards and to the expectations set forth in an SOW. Support is the act of managing and maintaining that device, system, or application after initial setup or deployment to ensure that reliability, availability, and performance continue to meet expectations. This activity may be delivered remotely or onsite.

14. **Support Desk:** The act of providing common support desk functions, including ticket management, problem tracking, and SLA Management. Support Desk is inherent in all Service Provider services, as the Support Desk is the single point of contact for and issues or requests. One of the key functions of a Support Desk is proper triaging of a ticket (Incident or Service Request). This includes collecting good contact information for the user, ensuring understanding of the due date, and ensuring understanding of the Urgency and Impact of the ticket such that tickets are worked in the appropriate priority order, per the guideline in the table below.

Impact \ Urgency	Critical	High	Medium	Low	Informational
Patient Care or System Security Affecting	1	2	3	4	10
Multi-Organization	1	2	3	4	10
Single Organization	2	3	5	7	10
Department or Single Application	3	5	7	9	10
Single User or Department w/Workaround	4	6	8	10	10
No Impact	10	10	10	10	10

15. **Reporting:** The act of collecting and reporting data to be used for auditing or decision making. This data can be aggregated from many sources such as installed applications, hardware information, licensing, system availability, usages, ticketing statistics, etc. Such sources, along with the relevant schedule and formatting of reports, will be identified in an SOW.

16. **User Management:** The act of managing the user account lifecycle across key systems identified in an SOW. The practice may include the creation, termination, and status changes of individual user accounts, including the management of groups and permissions. This may also include the creation and management of role groups and the leveraging of those groups for access to different systems.

Technical Services

Technical Services: The purpose of the Technical Services practice is to have an avenue to deliver labor to Client when the scope of work cannot be fully defined due to unknown complexity or unclear definition. Following execution of an SOW, Technical Services work will be completed as mutually agreed upon between Client and Service Provider. Whenever possible Service Provider will provide approximate estimates of labor when undertaking Technical Services work, however Technical Services work is inherently unpredictable and will necessarily be billed on a "time and materials" basis. Examples of Technical Services work may include implementation support for CRM, ERP, or other line of business applications or services; security remediation; technical consulting, etc. It may also include managing support requests on behalf of Client with third-party support entities such as line of business application vendors, connectivity providers, cloud service providers, etc.

Product Resale

1. **Hosted Backup Storage:** Backup storage is used to provide an offsite storage location hosted by Service Provider for long term retention of backups with the intention of protecting backups from a local disaster.

2. **Product Resale:** The act of quoting and procuring hardware, software, support, and licensing on behalf of Client utilizing Service Provider's procurement channels.

Professional Services

1. **Administration:** Administration is the act of configuration or setup of a device, system, or application to vendor-recommended standards, and the expectations set forth in an SOW.

2. **Deployment:** The act of provisioning devices, systems, applications, or services identified in an SOW for use within an organization. This may include the unboxing, imaging, configuration, application installation, updating, user data migration, and setup of a device for an end user, with the intention of minimizing user impact and downtime. This may also include the installation of any physical devices, such as network equipment, IT infrastructure, physical servers, etc.

3. **Design:** The act of designing a solution, service, device, or technology to meet both current and future performance and capability needs of the Client.

4. **Discovery:** The act of inventorying and documenting Client's environment with the intent of either reporting the current state of the environment to the Client or as an act of onboarding a new Client. Items identified in onboarding may include but are not limited to network segments, systems, devices, and patch levels.

5. **Migration:** The act of moving a device, application, or service from one environment or system to another, maintaining the same level of functionality unless otherwise set forth in an SOW. This may be as-is migrations, or the migration may also include migration to newer platforms or technologies.

6. **Project Management:** The act of providing project oversight to ensure that projects are delivered on time and on budget, and that deliverables to the Client meet the expectations established in an SOW. Project Management typically also includes communication with the Client regarding the project status as well as assisting with the removal of impediments to project completion.

RESPONSIBILITIES AND TECHNICAL REQUIREMENTS.

A. Security Incident Notification and Procedure. Managed IT Services alone are not intended to be a data security or data security monitoring service. However, in the event Service Provider becomes aware of an actual or potential unauthorized access, penetration, or acquisition of Client Data that Service Provider reasonable determines could compromise the security, confidentiality, or integrity of Client Data ("Security Incident") Service Provider shall:

1. *Notice*. Notify Client of any Security Incident, known to and confirmed by Service Provider, as soon as practicable, but no later than twenty-four (24) hours after confirmation by Service Provider of a Security Incident.

2. *Point of Contact*. Provide Client with the name and contact information for a representative of Service Provider who shall serve as Client's primary point of contact and shall be available to assist Client in responding to the Security Incident.

3. *Response*. Following Service Provider's notification to Client of a Security Incident, the Parties shall coordinate with each other to investigate the Security Incident. Service Provider agrees to reasonably cooperate with Client in Client's handling of the matter, including: (i) assisting with any investigation; (ii) providing Client with access to the equipment and facilities affected; and (iii) making available all relevant records, logs, files, data reporting and other materials relating to Client Data required by Client to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Client.

4. *Mitigation*. Service Provider may, at Client's expense, take commercially reasonable steps to prevent any further Security Incident in accordance with applicable privacy rights, laws, regulations, and standards.

5. *Liability*. Client shall be solely responsible for and agrees to reimburse Service Provider for Service Provider's costs incurred in connection with any services provided by Service Provider relating to any Security Incident, including costs incurred pursuant to paragraph 3 and 4 above, at Service Provider's then-current hourly rate, and all costs of third-party experts or specialists, remediation to affected persons, ransomware, or otherwise. Managed Services are not a data security, data breach prevention, or data breach monitoring service and Service Provider shall not be liable to Client in any way relating thereto.

6. *Third-Party Disclosure*. Unless otherwise required by applicable law, Service Provider shall not inform any third-party, other than its insurance carrier or retained third-party experts, lawyers, or consultants of any Security Incident without first obtaining Client's prior written consent. Further, Service Provider agrees that Client shall have the sole right to determine: (i) if third-party experts or specialists are retained by Client; (ii) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Client's discretion; and (iii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Notwithstanding the foregoing, in the event Service Provider receives a written opinion of a third-party attorney that Service Provider is required by law to provide any

notice or report of a Security Incident, or take any other action, then Service Provider may provide such notice or report, or take such action, without breach of the Agreement.

B. Client Responsibilities.

1. *Hardware, Software, and Third-party Services.* Client shall be responsible for all costs associated with any hardware, software, or third-party services required or used as part of the Managed Services, including any variable technology services (as set forth in the SOW) that may fluctuate from time-to-time based on Client's IT environment.

2. *Access*. Client shall ensure that Service Provider has access to each Client location, either onsite or remotely, as well as to any relevant devices, systems, or applications as necessary for Service Provider to provide the Managed Services, including all permissions, clearance, and security.

3. *On-Site Obligations.* Where the performance of the Managed Services requires Service Provider to provide Services on-site at Client's location, Client shall provide, at no cost to Service Provider, full and safe access to Client's facilities. Client shall provide suitable and adequate working space for Service Provider, including but not limited to parking, adequate light, heat and ventilation, Internet access, necessary equipment, electrical outlets, and telephone facilities.

4. *Cooperation.* Client shall cooperate with and follow instructions from Service Provider given in furtherance of the Managed Services or as otherwise necessary in order to address any problems relating to the Managed Services. Any delay in implementation, delivery, or completion of services caused by Client's actions or inactions may result in the assessment of additional fees, in Service Provider's reasonable determination.

5. *Third-party Warranties.* As part of the performance of the Managed Services, Service Provider may be required to access hardware or software that is not manufactured or licensed by Service Provider. Client is solely responsible for ensuring that Service Provider's access to such hardware or software does not adversely affect or void any third-party warranties or violate any software license agreement relating to the same. Client acknowledges and agrees that Service Provider is not responsible for any third-party warranties and extends no warranties of its own related to any services, equipment, or software provided to Client. Service Provider does not extend any warranty to Client; however, to the extent there are any original equipment manufacturer ("OEM") warranties that are intended by the OEM to be passed through to Client, Service Provider will make reasonable efforts to pass such warranties through to Client.

6. *Acceptance*. Upon completion or delivery of a Technical or Professional Service, Service Provider shall deliver a notice of completion to Client. Unless Client delivers written notice to Service Provider within five (5) days (or other time period set forth in the SOW) of the delivery of Service Provider's notice that the Service is not properly functioning, Client shall be deemed to have accepted the Service as of the notice date and the Service Term (if applicable) and billing shall commence. In the event Client notifies Service Provider within the aforementioned time frame that the Service is not functioning properly, then Service Provider shall correct any deficiencies in the Service and deliver a new notice of completion, after which the process stated herein will be

repeated, until the Service is accepted. Upon acceptance, unless stated otherwise in an applicable SOW, Service Provider's obligations related to the accepted Service cease.

7. *Notification.* Client shall provide timely notifications of any changes or updates to Client's IT policies and procedures, strategic priorities, business requirements, or any variable technology service (as set for the SOW), including onboarding and offboarding of personnel, that may impact the delivery, quantity, or cost of the Managed Services.

8. *Client Technical Requirements*. Client's location and IT infrastructure and environment must meet the minimum technical requirements listed below ("Minimum Standards"), unless otherwise provided in the SOW. All costs required to bring Client's environment to the Minimum Standards are the sole responsibility of Client.

i. All devices shall be running currently supported, industry standard operating systems and applications;

ii. All desktop software used by Client shall be genuine, licensed and vendor-supported;

iii. All servers, desktops, notebooks/laptops, and email shall have a currently licensed, up-to-date, industry standard (or better), and vendor-supported antivirus and anti-spam solution;

iv. A currently licensed, vendor-supported, industry standard (or better) backup or similar solution;

v. A currently licensed, vendor-supported, industry standard (or better) hardware firewall between the Client's network and the Internet;

vi. An active Internet subscription service, power, and other cabling sufficient for Service Provider to provide the Service as determined in its reasonable discretion;

vii. All hardware and software used by Client must be maintained under a valid contract or vendor support plan; and

viii. Compliance with Service Provider's fundamental security standards, as updated from time-to-time.

In the event Client does not meet the Minimum Standards, or a change in third-party software or systems materially changes Service Provider's delivery of the Services, any or all of the following may apply at Service Provider's discretion: (a) Service Provider shall be relieved of its obligations hereunder; (b) additional charges shall apply; and/or (c) Client shall be required to purchase any necessary hardware, software or equipment to meet such Minimum Standards and perform such other tasks as are required to ensure it complies with the Minimum Standard to Service Provider's reasonable satisfaction prior to Service Provider performing the Services hereunder.