REQUEST FOR LEGAL SERVICES

To: County Attorney's Office
Attention: Noah Milov

From: Grant Ewert, Drawer No. AS04

Dept: IT Ext. 7580

Date: 03/17/2025

Request (in detail):
Please review the attached contract between the county and CDW-G. This will be for managed professional services to follow the divestiture project that we are completing with them. That divestiture SOW was recently reviewed and signed by the County Manager.

Please indicate any time limits involved and attach all necessary documentation.

For County Attorney office use only:
Assign to: Noah Date: 3/17/25

County Attorney Project No.: 25-232
Logged out: 4/3/25

- Changes on Pg 11

STATEMENT OF WORK

Project Name:	Polk County Clerk of Courts- Managed 365 Services	**Seller Representative:** Anson Hira +1 (689) 2726088 anson.hira@cdwg.com
Customer Name:	Polk County, A Political Subdivision of the State of Florida	
CDW Affiliate:	CDW Government LLC	
Date:	April 30, 2025	**Solution Architect:** James Williams
Drafted By	Michelle Caron	

This statement of work ("**Statement of Work**" or "**SOW**") is made and entered into on the last date that this SOW is fully executed as set forth below ("**SOW Effective Date**") by and between the undersigned, CDW Government LLC ("**Provider**," and "**Seller**,") and Polk County, A Political Subdivision of the State of Florida ("**Customer**," and "**Client**,").

This SOW shall be governed by that certain Sourcewell Vendor Agreement 071321#CDW between CDW Government LLC and Sourcewell effective November 13, 2021 (the "**Agreement**") If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement.

PROJECT DESCRIPTION

PROJECT SCOPE

The term "**Services**" shall collectively refer to those managed services purchased under this SOW and as detailed in the **Exhibits.**

SOW LIST OF EXHIBITS ARE INCORPORATED AS PART OF THIS SOW HEREIN:

- Exhibit A – Recurring Services Fees
- Exhibit B – SLA Performance Standards
- Exhibit C - Customer Provided Infrastructure
- Exhibit D – Services Roles and Responsibilities
- Exhibit E – Seller Glossary of Defined Terms
- Exhibit F - Extended End of Life Support

Provide monitoring, daily operations, management, administration, incident support, service request support, problem management, thought leadership, architectural guidance, reporting, change management and engagement management services for the following Microsoft 365** tenant workloads:

1. Microsoft Exchange Online (EXO)
2. Microsoft EntraID (Azure Active Directory (AAD)) identity and access management*

3. Microsoft SharePoint Online (SPO)
4. Microsoft 365 Microsoft Security and Compliance* (Microsoft Defender Security and Microsoft Purview Compliance) *
5. Hybrid – Exchange On-premises Servers
6. Hybrid – Entra Connect

**As it relates to the in-scope Microsoft 365 workloads, native functionality*

*** Microsoft may rename and rebrand workloads. This service catalog reflects workload names and functionality at the time of signing and applies to functionality that remains unchanged regardless of workload brand name changes.*

Provider to focus on the in-scope responsibilities and do not include end user help desk services (first call to help desk, hands-on device support, client application support).

Below is the Service Catalog for services that Provider will provide, and the items listed under Provider are in-scope for Provider to complete. The items listed under the Client are out-of-scope for Provider and the Client is responsible for those items.

Any services not listed or not included as in-scope are considered out-of-scope.

SERVICE CATALOG

SCOPE OF SERVICES

Responsibility Description for Microsoft 365		Client	Provider
0	**On-Boarding – Microsoft 365 Services**		
0.1	Provide architectural and environmental information regarding the Microsoft 365 environment	✓	
0.2	Review architectural and environmental information regarding the Microsoft 365 environment		✓
0.3	Add/Remove Provider resources in the Client Microsoft 365 technical contact distribution list	✓	
0.4	Provide Provider resources administrator roles assigned to access and manage the Client's Microsoft 365 tenant. These roles are as follows, but are not limited to: • Compliance Administrator role • Directory Reader role • Exchange Admin (Organizational Management) role • Global Reader role • Groups Admin role • Message Center privacy reader role • Message Center reader role • Reports Reader role • Search Admin role • Security Administrator role • Security Reader role • Service Support Admin role • SharePoint Admin role • User Admin role Client will provide Provider sufficient access to perform in-scope tasks and functions.	✓	

0.5	Provide federation of Client Microsoft Teams domains with Provider Microsoft Teams domains	✓	
0.6	Provide governance plan for each Microsoft 365 workload	✓	
0.7	Review governance plan for each Microsoft 365 workload		✓
0.8	Provide current Client runbook for administrative processes	✓	
0.9	Review Client runbook for administrative processes		✓
0.10	Provide current Client security posture for Microsoft 365. This includes any reports created from 3rd-party vendors or products which help Provider to gain clarity on the current status of the Microsoft 365 tenant.	✓	
0.11	Review current Client security posture documents for Microsoft 365 tenant		✓
0.12	Provide Client end user provisioning, deprovisioning, and update process information	✓	
0.13	Review Client end user provisioning, deprovisioning, and update process information		✓
0.14	Define and document action plan to become compliant for Managed Services	✓	✓
0.15	Define and document escalation paths and processes	✓	✓
0.16	Define and document support methods, framework, and processes	✓	✓
0.17	Provide Provider with Microsoft Unified/Premier, Cloud Solution Provider (CSP), Signature or other Support Agreement information	✓	
0.18	Provide Provider access to contact Client's Microsoft Unified/Premier, Cloud Solution Provider (CSP), Signature or other Support on behalf of Client (designee on behalf of Client)	✓	
0.19	Generate Microsoft partner admin access request to administer Client Microsoft 365 tenant		✓
0.20	Grant Provider Microsoft partner access to administer Client Microsoft 365 tenant	✓	

Responsibility Description for Microsoft 365		**Client**	**Provider**
1	**Administration – Microsoft Exchange Online/Exchange Hybrid**		
1.1	Configure and manage Microsoft Exchange Online (EXO) with PowerShell		✓
1.2	Configure and manage Microsoft Exchange Online (EXO) with Exchange Admin Center		✓
1.3	Configure and manage permissions for administrative roles and groups		✓
1.4	Configure and manage end user permissions		✓
1.5	Configure and manage mail routing between domains		✓
1.6	Configure and manage conditional mail routing and transport rules		✓
1.7	Configure and manage inbound partner safe list		✓

1.8	Configure and manage Simple Mail Transfer Protocol (SMTP) relay through Microsoft Exchange Online (EXO)		✓
1.9	Configure and manage Microsoft Exchange Online Protection (EOP) anti-spam and anti-malware protection		✓
1.10	Configure and manage Quarantine settings		✓
1.11	Configure and manage address book policies		✓
1.12	Configure and manage offline address book		✓
1.13	Configure and manage user mailboxes		✓
1.14	Configure and manage resource mailboxes		✓
1.15	Configure and manage deleted mailbox recovery		✓
1.16	Configure and manage user self-service deleted item recovery		✓
1.17	Configure and manage archive mailboxes		✓
1.18	Configure and manage archiving rules and policies		✓
1.19	Configure and manage Microsoft 365 Groups		✓
1.20	Configure and manage distribution groups		✓
1.21	Configure and manage external contacts		✓
1.22	Configure and manage Public Folders		✓
1.23	Configure and manage mailbox forwarding		✓
1.24	Configure and manage mailbox sharing		✓
1.25	Configure and manage organization relationships/federated sharing		✓
1.26	Configure and manage message tracing		✓
1.27	Configure and manage eDiscovery and Compliance Manager Admin Roles and permissions		✓
1.28	Configure and manage In-Place Hold and Litigation Hold settings in Exchange Admin Center		✓
1.29	Configure and manage journaling rules for external data management		✓
1.30	Configure and manage content search configurations		✓
1.31	Configure and restrict ActiveSync policies for mobile devices		✓
1.32	Provide end user support (Client applications on devices)	✓	
1.33	Manage user on-boarding and off-boarding processes and tasks for email access	✓	
1.34	Manage and support user Personal Storage Table (PST) archive files for Outlook	✓	
1.35	Hybrid - Apply Microsoft Exchange Server On-Premises Cumulative Updates		✓

1.36	Hybrid - Apply Microsoft Exchange Server On-Premises Security Updates		✓
1.37	Hybrid - Configure and manage hybrid email routing for Exchange Hybrid Organizations		✓
1.38	Hybrid - Manage recipient attributes and Globally Unique Identifiers (GUIDs) for identities synchronized from Active Directory (AD) to Entra ID		✓
1.39	Hybrid - Configure and manage Exchange Distribution Groups connected to AD synced groups		✓
1.40	Hybrid - Configure and manage user, resource and shared mailboxes connected to AD synced identities		✓
1.41	Hybrid - Troubleshoot email routing through Simple Mail Transfer Protocol (SMTP) relay either through Microsoft Exchange Online (EXO) or Exchange Server On-Premises		✓

Responsibility Description for Microsoft 365		**Client**	**Provider**
2	**Administration – Microsoft Entra ID (Formerly Azure Active Directory) (For In-Scope Microsoft 365 Workloads)**		
2.1	Create and delete user accounts (user on-boarding and off-boarding)		✓
2.2	Manage User Licenses (assign & unassign user licenses)		✓
2.3	Reset user passwords	✓	
2.4	Configure and manage Self Service Password Reset and custom banned password list		✓
2.5	Configure and manage Business-to-Business (B2B) guest access permissions & organization configuration in Client tenant		✓
2.6	Configure and manage Entra ID security groups		✓
2.7	Configure and manage Entra ID role assignments		✓
2.8	Configure and manage Multi-Factor Authentication (MFA) methods in Entra ID		✓
2.9	Provide conditions and requirements to enforce with Conditional Access (CA) policies	✓	
2.10	Configure and manage Conditional Access (CA) policies		✓
2.11	Configure and manage Entra ID Application registrations for Single Sign-On (SSO), acting as an Identity Provider for cloud applications. (Only applications that are natively supported for Entra ID can be configured. Configuration of the 3rd party service Provider/application, or application development, are not in-scope.)		✓
2.12	Hybrid - Configure and manage Active Directory Domain Services (ADDS) security groups	✓	
2.13	Hybrid - Configure and manage Entra Connect (AD Connect)		✓
2.14	Hybrid - Configure and manage Entra Connect (AD Connect) user roles and permissions for Microsoft 365		✓

2.15	Hybrid - Troubleshoot issues with object synchronization between Active Directory (AD) and Entra ID using Entra Connect (AD Connect)		✓
2.16	Hybrid - Configure and manage On-Premises Active Directory (AD) users and security groups related to Microsoft 365 applications.		✓
2.17	Hybrid – Apply Microsoft Cumulative Updates (CU) and security patches for Entra Connect (AD Connect)		✓
2.18	Hybrid –Configure and manage Self Service Password Reset (SSPR) with writeback to Active Directory	N/A	N/A
2.19	Hybrid Identity Management - Configure and manage Active Directory Federation Services (AD FS)	N/A	N/A

Responsibility Description for Microsoft 365		**Client**	**Provider**
3	**Administration – Microsoft SharePoint Online**		
3.1	Perform Site Governance per Client-provided governance plan		✓
3.2	Configure and manage SharePoint Site URL		✓
3.3	Configure and manage standard sites		✓
3.4	Configure and manage standard document libraries		✓
3.5	Configure and manage standard Lists		✓
3.6	Configure and manage internal user access and assignments to standard sites		✓
3.7	Configure and manage internal user access and assignments to standard document libraries		✓
3.8	Configure and manage internal user access and assignments to standard Lists		✓
3.9	Configure and manage external sharing policy		✓
3.10	Configure and manage external user access and assignments to standard sites, document libraries and lists		✓
3.11	Configure and manage Microsoft SharePoint Online (SPO) standard Themes	N/A	N/A
3.12	Configure and manage Microsoft SharePoint Online (SPO) standard Web Parts for sites	N/A	N/A
3.13	Configure and manage deleted Microsoft SharePoint Online (SPO) sites within retention period		✓
3.14	Configure and manage custom sites templates, content placement, and intranet portals. **Note:** If the Client requires support from the Provider, all labor associated with task 3.14 counts towards and utilizes the quarterly consulting hours, up to the amount listed per this SOW.	✓	
3.15	Provide end user support (Client applications on devices)	✓	

Responsibility Description for Microsoft 365		Client	Provider
7	**Administration – Microsoft Defender for Office 365 Security and Microsoft Purview Compliance (For In-Scope Workloads, As Applicable)**		
7.1	Configure and maintain Identity and Authentication Alerts		✓
7.2	Configure and manage Microsoft 365 message encryption		✓
7.3	Provide requirements for Data Loss Prevention (DLP) Policy, Data Classification Policy, Retention and Labeling Policy, Sensitivity Labels	✓	
7.4	Configure and manage Data Loss Prevention (DLP) Policy, Data Classification Policy, Retention and Labeling Policy, Sensitivity Labels		✓
7.5	Configure and manage Purview Information Protection		✓
7.6	Configure and manage PKI Certificate Authorities and certificates	✓	

Responsibility Description for Microsoft 365		Client	Provider
8	**Monitoring And Reporting (For In-Scope Workloads, As Applicable)**		
8.1	Monitor and report according to standard Provider monitoring plan for Microsoft 365		✓

Responsibility Description for Microsoft 365		Client	Provider
9	**System Maintenance (For In-Scope Workloads)**		
9.1	Coordinate system configuration updates and management	✓	✓
9.2	Coordinate planned outages	✓	✓
9.3	Communicate outages to users	✓	
9.4	Backup and restore of data using Third Party Vendor software/tools	✓	
9.5	Perform Third Party Vendor Integration escalation support for Microsoft 365 integrated solutions	✓	
9.6	Provide end user support and training on modifications resulting from any upgrades, configuration or system updates or changes	✓	

Responsibility Description for Microsoft 365		Client	Provider
10	**Cloud Solutions Provider (CSP), Microsoft Premier, or Unified Support Management for Microsoft 365 In-Scope Workloads**		
10.1	Create Incidents and escalations as necessary		✓
10.2	Create Defect escalations as necessary		✓
10.3	Create Service Requests and escalation as necessary		✓

Responsibility Description for Microsoft 365		Client	Provider
11	**Operational Runbook (For In-Scope Workloads)**		
11.1	Provide information on new processes/changes made to existing Client organizational procedures/processes as soon as approved by Client organization.	✓	
11.2	Update information on new processes/changes made to existing Client organizational procedures/processes		✓
11.3	Document changes to the Microsoft 365 environment and related configuration information		✓
11.4	Document ticket escalation path and process information		✓
11.5	Document production support process information		✓
11.6	Document operational information		✓

Responsibility Description for Microsoft 365		Client	Provider
12	**Consulting Services**		
12.1	Provide up to 30 hours/quarter of consulting services for out-of-scope M365 related workloads and related solutions. In addition, the Service Catalog Section 3.14 will utilize these hours.		✓

ADDITIONAL TERMS, LIMITATIONS AND DISCLAIMERS

1. Provider may change all or any portion of the Provider's equipment used to provide the Services ("Provider Infrastructure") at any time if Provider, in its sole discretion, determines such change is necessary or desirable, but Provider agrees to perform modification(s) in a manner that does not result in any permanent, substantial, materially adverse alteration to the Services provided to Customer under this SOW.
2. Notwithstanding anything to the contrary in the Agreement, the Parties acknowledge and agree that Provider may subcontract some or all of the Services, provided: (i) Provider ensures that subcontractors strictly comply with Provider's obligations contained within this SOW;(ii) any such subcontractor enters into a nondisclosure agreement with Provider containing terms substantially similar to the confidentiality provisions contained in the Agreement; and (iii) Provider remains responsible for the performance of any such subcontractors.
3. Notwithstanding anything to the contrary in the Agreement, subject to the limited rights expressly granted hereunder, Provider reserves all rights, title and interest in and to the Services, including all related systems and intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein. Provider shall have a royalty-free, worldwide, transferable, sublicensable, irrevocable, perpetual license to use, modify, and/or incorporate into the Services any suggestions, enhancement requests, recommendations or other feedback provided by Customer, relating to the operation of the Services.
4. Provider does not warrant that the Services will be uninterrupted, error-free, virus-free, or completely secure. The service level credits referred to herein shall be Seller's sole liability and Customer's exclusive remedy for interruptions, delays, impairments, inadequacies, or other defects in service with regard to any and all of the services.
5. Provider shall not be liable for any loss or damage resulting from unsupported Client provided hardware or software (whether such lack of support results from Client's failure to maintain a current maintenance and support agreement with the applicable vendor or the vendor's failure to maintain support for any other reason). Failure of Client to maintain a current maintenance and support agreement with the applicable vendor for each of the Client provided hardware or software shall release Provider from any service level agreement ("SLA") or associated penalty resulting from a missed SLA,

its financial penalty, or grounds for breach as defined herein.

6. All support will be delivered remotely by Provider's global based delivery services.
7. Provider will use a Standard Customer Deployment method for network connectivity for accessing the Customers environment. Different connectivity methods will need to be scoped and may incur additional costs. One standard connection is designed for the scope of this SOW.
8. All devices in scope can be accessed through a single domain or an established trust is in place. If additional domain connections are required, this is subject to a price increase.
9. Customer will utilize Provider Customer Portal for ticketing. Provider will not work in nor utilize Customer ITSM tools (ticketing).

TERM AND TERMINATION

This SOW will be effective as of the last date that this SOW is fully executed by the parties ("SOW Effective Date") The Recurring Services will commence upon completion of onboarding, covering the period beginning on the Recurring Services Start Date, and continuing for an initial term of twelve (12) months (the "Initial Term"). This SOW may be renewed for additional one (1) year terms (each a "Renewal Term")subject to a signed Change Order by the parties at least thirty (30) days prior to the expiration of the Initial Term or the then-current Renewal Term.

The Initial Term and each one-year Renewal Term, if any, may be referred to herein individually as a "Service Term" or collectively as the "Service Terms.". Notwithstanding anything to the contrary in the Agreement, the Parties agree that the following represent the termination options relative to this SOW:

1. End of Service Term. Either Party may terminate this SOW effective as of the end of the then current Service Term, by providing written notice of such termination at least thirty(30) days prior to the expiration of the then current Service Term.
2. Breach. Either Party may terminate this SOW if the other Party materially breaches any of its representations, warranties, or obligations under this SOW and such breach is not cured within fourteen (14) days of breaching Party's receipt of written notice specifying the breach.

For any termination by Customer, the notice of cancellation must be accompanied by payment in full for all Services through the effective date of termination. In the event of any Convenience Termination by Customer, Customer's notice of cancellation must also be accompanied by payment of the applicable cancellation charge(s). The Parties agree that the cancellation charge(s) are in addition to any other fees or payments of any nature owed by Customer. Upon any expiration or early termination of this SOW, Customer will return to Provider and relinquish all use of any equipment, applications, software, IP addresses, or address blocks and any other property assigned to Customer by Provider in connection with the SOW Services.

In addition to its right to terminate as provided for herein, Provider may suspend all or part of Customer's access to the Services (i) if Customer is delinquent on payment obligations; (ii) upon receipt of a subpoena or law-enforcement request; or (iii) when Provider has a commercially reasonable belief that Customer has breached this SOW or that Customer's use of the Services poses an imminent security risk.

Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

GENERAL RESPONSIBILITIES AND ASSUMPTIONS

- Customer is responsible for providing all access that is reasonably necessary to assist and accommodate Seller's performance of the Services.
- Customer will provide in advance and in writing and Seller will follow, all applicable Customer's facility's safety and security rules and procedures.
- Customer is responsible for security at all Customer-Designated Locations; Seller is not responsible for lost or stolen equipment, other than solely as a result of Seller's gross negligence and willful misconduct.

- Customer acknowledges that in order to efficiently and effectively perform the Services CDW may need to collect information from Customer's systems by using software tools developed or used by CDW ("Tools"). In some cases, these Tools will need to be loaded onto the Customer's systems to gather necessary information, and CDW may also use them to make changes in the Customer's systems consistent with the agreed upon scope. Tools will be used only for purposes of performing the Services and will be removed or automatically deleted when CDW has completed use of them. Customer hereby consents to CDW's use of the Tools as set forth in this paragraph.

CONTACT PERSONS

Each Party will appoint a person to act as that Party's point of contact ("**Contact Person**") as the time for performance nears and will communicate that person's name and information to the other Party's Contact Person.

Customer Contact Person is authorized to approve materials and Services provided by Seller, and Seller may rely on the decisions and approvals made by the Customer Contact Person (except that Seller understands that Customer may require a different person to sign any Change Orders amending this SOW). The Customer Contact Person will manage all communications with Seller, and when Services are performed at a Customer-Designated Location, the Customer Contact Person will be present or available. The Parties' Contact Persons shall be authorized to approve changes in personnel and associated rates for Services under this SOW.

CHANGE MANAGEMENT

This SOW may be modified or amended only in a writing signed by both Customer and Seller, generally in the form provided by Seller ("**Change Order**"). Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

In the event of a conflict between the terms and conditions set forth in a fully executed Change Order and those set forth in this SOW or a prior fully executed Change Order, the terms and conditions of the most recent fully executed Change Order shall prevail.

PROJECT SCHEDULING

Customer and Seller, who will jointly manage this project, will together develop timelines for an anticipated schedule ("**Anticipated Schedule**") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning.

TOTAL FEES

The total fees due and payable under this SOW ("**Total Fees**") include both fees for Seller's performance of work ("**Services Fees**") and any other related costs and fees specified in the Expenses section ("**Expenses**").

Seller will invoice for Total Fees. Customer will pay invoices containing amounts authorized by this SOW in accordance with the terms of the Agreement. Any applicable taxes will be invoiced but are not included in any numbers or calculations. The pricing included in this SOW expires and will be of no force or effect unless it is signed by Customer and Seller within thirty (30) days from the Date listed on the SOW, except as otherwise agreed by Seller. Any objections to an invoice must be communicated to the Seller Contact Person within fifteen (15) days after receipt of the invoice.
This SOW may include multiple types of Services Fees; please reference below Services Fees section(s) for further details.

SERVICES FEES

Services Fees hereunder are FIXED FEES, meaning that the amount invoiced for the Services will be $5,950.00.

The invoiced amount of Services Fees will equal the amount of fees applicable to each completed project milestone (see Table below).

* Services Onboarding Fee will commence upon signature of this SOW

Milestone	Percentage	Fee
One time Services Onboarding Fee -MAS-Transition and Onboarding*	100%	$5,950.00
Totals	**100%**	**$5,950.00**

Expenses

All services under this SOW will be performed remotely; therefore, neither travel time nor direct expenses will be billed for this project.

Travel Notice

The parties agree that there will be no travel required for this project.

RECURRING SERVICES FEES

Customer has chosen to purchase the Services indicated in **Exhibit A** ("Recurring Services Fees") of this SOW and agrees to pay Provider the fees, charges, and other amounts indicated in Exhibit A of this SOW. Except as otherwise stated in this SOW, Provider and Customer agree to follow the billing and payment terms, conditions, and procedures set forth in the Agreement.

Customer agrees to maintain the monthly minimum commitment for the Services, if any, as indicated in the **Exhibit A**: Recurring Services Fees of this SOW. For the avoidance of doubt, Recurring Services Fees shall commence upon completion of onboarding and at the start of steady state ("Recurring Services Start Date"). The Recurring Services Start Date will be communicated and agreed upon subject to a signed Change Order by the Parties.

Customer will not be required to pay charges for Services initially invoiced more than 6 months after close of the billing period in which the charges were incurred. If Customer disputes a charge, Customer will provide notice to Provider specifically identifying the charge and the reason it is disputed within 6 months after the date of the invoice in which the disputed charge initially appears, or Customer waives the right to dispute the charge. The portion of charges in dispute may be withheld and will not be considered overdue until Provider completes its investigation of the dispute. Following Provider's notice of the results of its investigation to Customer, payment of all properly due charges must be made within ten (10) business days.

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the following locations ("**Customer-Designated Locations**")

Location	Address
Polk County, A Political Subdivision of the State of Florida	330 W Church St, FL 5, Bartow, FL 33830
Polk County, A Political Subdivision of the State of Florida-Main Office	255 N. Broadway, Bartow, FL 33830

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

CDW Government LLC	**Polk County, A Political Subdivision of the State of Florida**
By: Joel Jacob	By:
Name: Joel Jacob	Name:
Title: Mgr Managed Services	Title:
Date: May 2, 2025	Date:
Mailing Address:	Mailing Address:
200 N. Milwaukee Ave. Vernon Hills, IL 60061	330 W CHURCH ST FL 5, IT DEPT BARTOW, FL 33830-3760 Account Number: 9451663

EXHIBIT A

RECURRING SERVICES FEES

Managed Services MAS-Microsoft 365	Description	Monthly Recurring Services Fees*
Month 1 through 12	Monthly Service Fee	$8,450.00
	SOW Total	**$101,400.00**

Applicable taxes not included
The Managed Services Recurring charge shall be invoiced upon the Recurring Services Start Date and shall be invoiced monthly in advance for the remainder of the Term.

Customer may request Additional Services from Seller that could consist of Elastic Engineering services. Elastic engineering services shall be used, as needed, for out-of-scope Microsoft M365 services not mentioned in the service catalog. Additional Services are provided by Seller, subject to resource availability, and shall be charged at the rates set forth in the section below.

Elastic Engineering - Time and Materials Support - Hourly Rate*
Managed Services Engineering and Consulting - Time and Materials Support - $210.00 per Hour

*Units will be measured in 0.25-hour increments. Upon notice, the Seller may adjust the rate, provided that it remains fixed for at least six (6) months after the SOW Effective Date and then again for at least six (6) months after any subsequent adjustment.

a) Additional Fee. Customer shall pay Provider for services outside the scope of this SOW at the Time and Materials Support – Elastic Engineering and Consulting via Change Order as mutually agreed to. Provider will notify Customer if services are outside the scope of the SOW prior to performing the service.

b) Assumptions. All the fees referenced above are based upon the following assumptions and in the event any such assumption proves to be invalid or incorrect for any reason, Provider reserves the right to adjust such fees accordingly:

i. Customer will be responsible for timely paying in full any fees charged by any third-party software vendors for the right to run such software and Customer will timely obtain the effective right for Provider to run any such software and shall indemnify, defend and hold Provider harmless for any liability and any cost or expense incurred (including, without limitation, any attorneys' fees) as a result of its failure to timely obtain such an effective right; and

ii. Customer shall bear and satisfy all telecommunication costs relating to its network; and

iii. Provider shall not be liable for any loss or damage resulting from unsupported Customer provided hardware or software (whether such lack of support results from Customer's failure to maintain a current maintenance and support agreement with the applicable vendor or the vendor's failure to maintain support for any other reason). Failure of Customer to maintain a current maintenance and support agreement with the applicable vendor for each of the Customer provided hardware or software shall release Provider from any service level agreement ("SLA") or associated penalty resulting from a missed SLA, its financial penalty, or grounds for breach as defined herein; and

iv. Provider assumes the hardware environments sized by Customer as set forth in **Exhibit C** are of sufficient size, quality, capability and capacity to adequately handle Customer's data processing and workload requirements; and

v. Customer shall provide Internet connectivity on a 24 by 7 by 365 basis into Customer's business locations where Provider is providing services. Customer shall also monitor the status of these Internet connection(s) utilizing a combination of host-based and microprocessor-based network management systems to ensure Provider connection availability. Customer will not hold Provider responsible for any SLA or associated penalty resulting from a missed SLA, its financial penalty, or grounds for breach as defined herein resulting from Customer's failure to comply with this subsection (v); and

vi. Client shall provide, manage and own all licensing aspects of the Client solution environment, including software, platforms, hardware and applications.

EXHIBIT B
SLA -Performance Standards

The following Performance Standards apply to the attached Managed Services SOW ("Managed Operations" and "Managed Administration") and whose penalties will be assessed in the event of a Performance Standards violation. The maximum Performance Standard penalty for a given month is ten (10) percent of one (1) months' fee and violations for different Performance Standards within the same Service Area are not cumulatively penalized.

Service Area	***Incident Management – Impact Level-1***
Service Level Description	Ensure Priority/ Severity Level-1 Incidents impacting Customer are managed in the timeframe defined within this SLA.
Service Category	Incident Response Process
Target KPIs	**Time to Respond SLA:** Within 1 hour of Provider becoming aware of the incident, Provider will have a resource assigned to work the incident. **SLA – 95% incidents acknowledged/assigned within 1 hour**
Calculation	(#Priority/ Severity-1 Incidents Logged) minus (-) (#Priority /Severity-1 Incidents Exceeded) divided by (÷) (#Priority/Severity-1 Incidents Logged)
Trigger	If incident is discovered by Customer first, the point in time the incident is reported to the Provider Help Desk and issuance of a Provider incident ticket will be considered the trigger point. If incident is discovered by Provider first, the issuance of a Provider incident ticket by the Provider Help Desk will be considered the trigger point.
Transition Period	90 days from services start date
Measurement Interval	Monthly
Service Level Weight	3% of Base Monthly Service Fee

Service Area	***Incident Management – Impact Level-2***
Service Level Description	Ensure Priority/Severity Level-2 Incidents impacting Customer are managed in the timeframe defined within this SLA.
Service Category	Incident Response Process
Target KPIs	***Time* to Respond SLA:** Within 2 hour of Provider becoming aware of the incident, Provider will have assigned resources/team to work the incident. SLA penalties are based upon a minimum of 10 P2 incidents per month. **SLA – 95% incidents acknowledged/assigned within 2 hours**
Calculation	(#Priority/Severity-2 Incidents Logged) minus (-) (#Priority/Severity-2 Incidents Exceeded) divided by (÷) (#Priority/Severity-2 Incidents Logged)
Trigger	If incident is discovered by Customer first, the point in time the incident is reported to the Provider Help Desk will be considered the trigger point. If incident is discovered by Provider first, the issuance of a Provider incident ticket by the Provider Help Desk will be considered the trigger point.
Transition Period	90 days from services start date
Measurement Interval	Monthly

Service Level Weight	3% of Base Monthly Service Fee

Service Area	***Incident Management – Impact Level-3***
Service Level Description	Ensure Priority/Severity Level-3 Incidents impacting Customer are managed in the timeframe defined within this SLA.
Service Category	Incident Response Process
Target KPIs	**Time to Respond SLA:** Within 4 hour of Provider becoming aware of the incident, Provider will have assigned resources to work the incident. SLA penalties are based upon a minimum of 10 P3 incidents per month. **SLA – 95% incidents acknowledged/assigned in 4 hours**
Calculation	(#Priority/Severity-3 Incidents Logged) minus (-) (#Priority/Severity-3 Incidents Exceeded) divided by (÷) (#Priority/Severity-3 Incidents Logged)
Trigger	If incident is discovered by Customer first, the point in time the incident is reported to the Provider Help Desk will be considered the trigger point. If incident is discovered by Provider first, the issuance of a Provider incident ticket by the Provider Help Desk will be considered the trigger point.
Transition Period	90 days from services start date
Measurement Interval	Monthly
Service Level Weight	3% of Base Monthly Service Fee

Impact Level	Incident Impact
1 HIGH	**Emergency or Critical condition requiring immediate attention and resolution** A major impact to multiple components in the computing environment. A mission critical component is down. Significant and immediate business impact. A key business condition documented or identified by the Client is impacted. *Incident resolution will be initiated immediately and attention to the resolution of these incidents will be sustained around the clock until a temporary work around is in place or a permanent solution is implemented.*
2 MEDIUM	**Medium impact to Customer** Single critical business function is impacted (a workaround may be in place). Service or performance is degraded for multiple end users. A key component is severely degraded or in danger of failing. A key business condition documented or identified by the Client is degraded or in danger of being missed. *Incident resolution will be initiated immediately and attention to the resolution of these incidents will be sustained as deemed appropriate based on mutual agreement between Provider and Client until a temporary work around is in place or a permanent solution is implemented.*
3 LOW	**Low impact to Customer** Minor service components are down or failing. Batch processing has received failures (but critical batch processing can continue). Service or performance is degraded for a single user. Alternative method is being used with no business impact or service degradation.

Note: The Service Level Agreement or Objective clock will be paused or deferred when pending Customer or vendor feedback, or creating a change to resolve the incident

Performance Measurements Exceptions

Provider shall incur no liability for and, to the extent the following occur or directly impact Provider's performance, no failure to meet Performance Measurements shall result in Service Credit calculation for the Performance Measurements listed in this SOW:

a. Any acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike, or other labor disturbance; interruption of or delay in transportation; unavailability of or interruption or delay in telecommunications or third-party services; failure of third-party software; or inability to obtain power used in or equipment needed for provision of the Performance Measurement; or any other acts, omissions, events, or circumstances beyond Provider's reasonable control;
b. Failure to meet any Performance Measurement is prevented as a result of Customer's direct or indirect acts or omissions (or acts or omissions of other parties engaged or authorized by Customer), including without limitation: any alteration of the configuration of the environment being used by Customer that causes the Customer's platform to fail; and
c. Any downtime during Scheduled Maintenance (or Emergency Maintenance) on Provider provided software/hardware required to perform the Managed Services. PROVIDER will notify Customers of any Scheduled Maintenance to be performed.

Maintenance windows are required by Provider for any Provider owned or provided software/hardware ("Provider Infrastructure") that is leveraged to deliver any Infrastructure Service or Managed Service. These required maintenance windows will be removed from any Notice of Planned Maintenance and Planned Emergency Maintenance will be provided to Customer's designated point of contact by a method elected by Company (telephone, email or Customer portal). Provider will use best efforts to notify Customer in advance of any Unplanned Emergency Maintenance if conditions permit.

Preventative Maintenance – Normal maintenance activities that may or may not disrupt Service include:

a. Maintenance of which Customer is notified nine (9) days in advance; and
b. Maintenance that is performed during a standard maintenance window: Wednesdays from 12:01 am – 6:00 am and Sundays from 12:01 am – 8:00 am local time of the Provider Data Center in which maintenance is being conducted.

Planned Emergency Maintenance – Planned Emergency Maintenance required to remediate or prevent a degradation of or loss of service, or to complete a Customer incident requirement (all Incidents fall into this category SEV1, SEV2, SEV3) includes:

a. Maintenance of which Customer is notified twenty-four (24) hours in advance if conditions permit; and
b. Maintenance that is performed during a maintenance window any day from 12:01 am – 6:00 am local time of the Provider Data Center in which maintenance is being conducted.

Unplanned Emergency Maintenance – Unplanned Emergency Maintenance is required to remediate or prevent a loss or severe degradation of service. (SEV1, SEV2, SEV3)

EXHIBIT C

CUSTOMER PROVIDED SOLUTION ENVIRONMENT

THE SOLUTION ENVIRONMENT CONSISTS OF THE FOLLOWING CLIENT PROVIDED COMPONENTS

Solution Environment	**Provided by:**	**Used for:**
Microsoft Exchange Online Microsoft SharePoint Online Microsoft Entra ID (formerly Azure Active Directory) * for Microsoft 365 Microsoft Security and Compliance* (Microsoft 365 Defender Security and Microsoft Purview Compliance) **As it relates to the in-scope Microsoft 365 workloads, native functionality.* Hybrid Exchange On-premises Servers Entra Connect	The Microsoft 365 tenant is provided by the Client.	Messaging and Collaboration

EXHIBIT D

SERVICES ROLES AND RESPONSIBILITIES

GENERAL:

I. The current Client Microsoft 365 tenant environment is stable, issue free, and in good health.
II. Any Microsoft 365 tenant deployment and/or migration project has been completed, and the environment is in steady state, prior to on-going full managed services initiation.
III. The support covers one PROD Microsoft 365 tenant, owned and provided by the Client, with up to 330 Microsoft 365 G5 licenses.
IV. The support covers up to one (1) Exchange On-premises Hybrid instance and one (1) Entra Connect instance.
V. Client will own and provide all licensing related to Microsoft 365.
VI. Services are based on the capabilities that the Client Microsoft 365 licensing provided (licensing inclusions / SKUs.). If the Client licensing level does not include a certain capability, Provider cannot manage and support such capability.
VII. Provider will leverage Client provided vendor support agreements and associated licensing.
VIII. Client has a Microsoft support agreement. Provider will utilize the Client Cloud Solution Provider (CSP), Microsoft Premier, or Unified Support agreement. Client will designate Provider as a Customer representative for the support agreement.
IX. Client will grant Granular Delegated Admin Permissions (GDAP) through Microsoft Partner admin relationship requests.
X. Client will create Provider resource user accounts in the Client Microsoft 365 tenant. An appropriate license will be assigned to Provider resources by Client. Provider will not utilize guest accounts.
XI. Provider will use a combination of Lighthouse (Partner Center / GDAP) and Microsoft 365 user account administrator roles to access the Client tenant environment.
XII. Provider will follow Client Privileged Identity Management (PIM) processes.
XIII. Provider can access the Client Microsoft 365 environment from the Internet and will not require Client intranet access.
XIV. Provider services focus on Microsoft 365 tenant administration, management and support. Provider is not providing a Level-1 end user Help desk service. Client has an end user service desk that provides end user support. Client users will contact the Client Help Desk to report Incidents and Service Requests. The Client Help Desk will perform initial triage and support. The Client Help Desk will then escalate related in-scope items to Provider for follow up.
XV. Provider will utilize the Provider Managed Services ITIL processes.
XVI. Client will utilize the Provider defined Severity scale for Incidents.
XVII. Client will provide guidance and approval for change management related activities.
XVIII. Maximum of four normal or emergency change requests will be executed per month.
XIX. No technical change request (normal, standard, emergency or other) nor other technical changes will be executed during the last two weeks of contracted services.
XX. Security, governance, and compliance related activities will follow Client direction.
XXI. Provider will not have on-site personnel at Client locations.
XXII. All monitoring and reporting include using native and out of the box Microsoft 365functions. No third party tools will be deployed.
XXIII. Client provides Provider access to resources who can manage, configure and support Client responsible services.
XXIV. Client will be responsible for maintaining, managing and supporting the Client user endpoint related requirements, images and services. This includes mobile devices, tablets, laptops and desktops.
XXV. Deleted item restoration using Microsoft 365 native capabilities is constrained to Microsoft retention limits.
XXVI. Client will perform end user communication and training.
XXVII. Client has defined policies and processes for user related activities such as, but not limited to, end user on-boarding, off-boarding, and license assignments. Provider expects to be able to follow those policies as pertinent to in-scope items, and processes in performing related Microsoft 365 in-scope services.
XXVIII. Custom applications, migrations and solution changes are out of scope.

XXIX. Additional environments/solutions change the level of effort and will need to be evaluated. A Change Request would be created to change the scope of services.

XXX. The services do not include development (e.g., PowerApps and Power Automate).

XXXI. Consulting hours can be used to provide advisory services for out-of-scope Microsoft 365 workloads.

XXXII. Labor associated with task 3.14 "Configure and manage custom sites templates, content and intranet portals" will count towards the consulting hours (Service Catalog Section 12).

XXXIII. Consulting hours do not carry over quarter to quarter and cannot be pooled. There are no refunds for unused hours.

XXXIV. Provider is not liable for any failure of performance from any 3rd party including, but not limited to, Microsoft, customizations within the Power Platform, Power Platform Connectors and integrations.

XXXV. Provider User on-boarding and off-boarding tasks include only using Microsoft 365 tools.

XXXVI. Client will provide Provider resources Remote Desktop/PowerShell module access for Hybrid servers such as Exchange On-Premises Servers and/or Entra Connect Sync servers.

XXXVII. Client has the ability to fully restore Exchange On-Premises servers to the most recent version prior to the updates, patching and configuration changes.

XXXVIII. Client has the ability to fully restore Entra Connect Sync (Azure AD Connect) servers to the most recent version prior to the updates, patching and configuration changes.

XXXIX. Entra Connect (AD Connect) Sync will be configured to automatically apply updates and patching.

XL. Provider will consult the Client security team prior to applying Cumulative Updates (CU) and security patches. Client security team will provide approval prior to Provider applying such patches or updates.

XLI. Provider will target to apply future CUs within 60 days of release, but no sooner than 15 days of release date to ensure stability of such releases. Please note that this does not apply to the initial round of patching, CU, version upgrades and roll updates if the Client versions are currently down level. The first round of such work may require additional timelines to appropriately plan for them .Client will coordinate the patching, CU, version upgrades and roll updates with Provider. Provider will target to follow Microsoft recommendations regarding deploying security patches based on their Common Vulnerability Scoring System (CVSS) value and CU requirements.

EXCLUSIONS:

The following items are Client responsibility and are thus out-of-scope for Provider with Microsoft 365 services. Provider assumes the Client managed and supported items are fully functional, stable and error free:

i. Tier 1 End User Support services (first call to Help Desk, End User Application Support, Hands-on support).
ii. Licensing.
iii. Vendor support agreements.
iv. Creating and modifying SharePoint Online content, including graphics.
v. End user endpoints, workstations, mobile devices and desktops, including images, applications on endpoints, hardware, installations and support.
vi. Telephony telecom, hardware, Voice Over Internet Protocol (VOIP), Voice Systems, Calling Plans, Voice and Data Services.
vii. End user managed Outlook functions (e.g., personal groups), Personal Storage Table (PST), Outlook installations and local end user mail archives.
viii. Web content filtering and package inspection.
ix. Custom and 3rd party applications, solutions, integrations, and add-ons.
x. Disaster Recovery (DR), including testing, configurations, set up and recovery efforts.
xi. Backup and restore solutions and processes.
xii. Legal compliance audits.
xiii. Non-Microsoft Security (e.g., Proofpoint), Anti-malware and anti-virus solutions and Identity solutions (e.g., Okta, SailPoint).
xiv. Network, Domain Name System (DNS), Load balancers, Operating Systems (OS), Distributed File System (DFS), security appliances, Dynamic Host Configuration Protocol (DHCP) Internet Protocol (IP) address allocation and other hardware and infrastructure components.
xv. Development and related testing Quality Assurance (QA).
xvi. Public Key Infrastructure (PKI) and Public Certificate Authority (PCA).
xvii. Monitoring tools.

xviii. Training for users, developers and administrators.
xix. Any deliverable, solution or work product not listed in the Service Catalog as in-scope.

SERVICE MANAGEMENT

General Services and Responsibilities

Standard Support Connectivity Assumptions

Account Management Responsibilities

Responsibility Description	Client	Provider
Status Reporting & Meetings		
Conduct regularly scheduled status meetings as agreed upon by both parties		✓
Implement service level objectives and performance reports		✓
Prepare monthly service level/performance reports		✓
Provide analysis of monthly reports and service level achievement/performance		✓
Provide feedback regarding analysis/results of monthly reports and historical trends	✓	
Determine reason(s) for failing to meet defined SLAs and present to Client		✓
Provide feedback regarding any failure(s) to meet defined SLAs as presented by Provider	✓	
Determine appropriate measures/compensation actions that are a result of a failure to meet defined SLAs		✓
Provide feedback regarding measures/compensation actions that are a result of a failure to meet defined SLAs as presented by Provider	✓	
Provide appropriate reporting required for supporting SLAs		✓
Schedule and conduct regular executive review with client stakeholders upon mutually agreed upon timeframe and schedule		✓
Report in a timely and accurate manner on progress toward delivery or resolution of Provider action items		✓
Report in a timely and accurate manner on progress toward delivery or resolution of Client action items	✓	
Implement Provider action items agreed upon and resulting from Client support meeting		✓
Implement Client action items agreed upon and resulting from Client support meeting	✓	
Contract Management		
Ensure performance of Provider' obligations		✓
Ensure performance of Client's obligations	✓	
Oversee performance of Provider' obligations	✓	
Provide constructive feedback regarding performance of Provider' obligations	✓	
Take appropriate measures to meet Client's expectations regarding Client's constructive feedback		✓
Maintain documentation and procedures regarding services provided to Client		✓

Responsibility Description	Client	Provider
Approve documentation and procedures relative to Client services	✓	
Document modifications (SOW Change Requests) to contract and provide to Client for approval and signature		✓
Provide Client signature regarding documented modifications to SOW	✓	
In Scope Services		
Surface Client initiated incidents and service requests	✓	
Surface Provider initiated incidents and service requests		✓

Identify tasks required to complete activities		✓
Provide input toward identifying tasks required to complete activities	✓	
Approve list of identified tasks required to complete activities	✓	
Estimate and manage Client resources required to complete activities	✓	
Estimate and manage Provider resources required to complete activities		✓
Create and execute implementation plans in accordance with agreed upon processes		✓
Review and approve Provider' implementation plans	✓	
Record and report status and/or results of initiative's activities		✓
Out of Scope Services		
Initiate a written request to provide out of scope services (with a description of the request).	✓	
Identify tasks to the level of major milestones and deliverables required to complete projects or activity		✓
Provide input toward identifying tasks required to complete project or activity	✓	
Approve list of identified tasks required to complete project or activity	✓	
Estimate and manage Client resources required to complete project or activity	✓	
Estimate and manage Provider resources required to complete project or activity		✓
Review Provider' plans and cost quote	✓	
Provide verbal approval of scope regarding work modifications	✓	
Document project or activity via creating a Change Request to be signed/executed by Client in accordance with agreed upon processes		✓
Provide Client signature regarding documented Change Request and corresponding cost	✓	
Create and execute implementation plans in accordance with agreed upon processes for the items as described in the Client signed and approved Change Request		✓
Record and report results and/or status of initiative's activities		✓
Transition to Managed Application Services		
Initiation		
Assign a Client Executive Sponsor and a Project Coordinator	✓	
Create and maintain Transition Project Schedule		✓
Provide requested transition related information	✓	
Schedule weekly transition status meeting with stakeholders		✓
Attend weekly transition status meeting	✓	✓
Discovery & Knowledge Transfer		
Schedule discovery and knowledge transfer sessions with transition project stakeholders		✓
Attend discovery and knowledge transfer sessions with transition project stakeholders	✓	✓
Provide necessary documentation related to supporting and managing the application platforms and environments requiring Provider support, as applicable for the in-scope solution. This includes, but is not limited to:	✓	

Responsibility Description	Client	Provider
Architectural diagrams Environmental information System access information Procedures and processes pertaining to in-scope services Maintenance procedures Administration procedures Operational procedures Runbooks Process flows Escalation and callout processes Change Management Procedures		
Provide Provider with administrative user credentials for the application platforms and environments requiring Provider support	✓	
IT Service Management (ITSM) Setup – Provider ServiceNow		
Provide Client Point of Contacts for Provider ServiceNow access (web portal, reports, incident / service request creations)	✓	
Create and configure Provider ServiceNow user accounts for the Client		✓
Configure Provider ServiceNow dashboard and standard reports		✓
Train Client on the use of the Provider ServiceNow incident and service request management tool		✓
Review Provider Application Managed Services ITSM Process Incident Management Service Request Management Change Management Release Management Problem Management		✓
Create Provider Escalation & Callout document for the supported application platforms and environments		✓
Add the Configuration Items to Provider ServiceNow		✓
Provide Client with the Provider Escalation documentation		✓
Provide Provider with the Client Escalation documentation	✓	
Go-live Preparation		
Approve the Managed Services "Go Live" date identified in the transition project schedule	✓	
Ensure Client transition items have completed	✓	
Ensure Provider transition items have completed		✓
Complete go-live handoff to Provider	✓	
Closure		
Perform post-transition review process		✓
Provide input and feedback regarding post-transition review process	✓	
Relationship Management		
Provide oversight regarding account activities		✓
Initiate and host status/Client support meetings at a mutually agreed upon timeframe		✓
Assign Client resource(s) that will review and provide approval for all Client related changes	✓	
Work with Client to review and obtain approval for all Client related changes		✓
Provide approval for all Client related changes	✓	
Provide the communication between Client and Provider		✓
Provide critical input and communication to allow activities to be completed within a timely manner between Client and Provider	✓	

Provide and maintain a single point of contact for escalating reporting items and ITSM activities	✓	✓

Responsibility Description	Client	Provider
Address any billing related issues or concerns of Client		✓
Address any billing related issues or concerns of Provider	✓	

Operations Center / ITSM Tools

Responsibility Description	Client	Provider
Log all Client calls via Provider ServiceNow ticketing system, assign severity and monitor progress of incident service requests		✓
Submit Client tickets via the Provider Operations Center Phone Service	✓	
Submit Client web tickets via Provider ServiceNow ticketing system	✓	
Triage and escalate incidents and Service Requests to the appropriate technical resource for resolution or route incident ticket to appropriate service provider or on-call Client analyst		✓
Establish and enforce security standards and guidelines	✓	
Follow Client publicized security standards and guidelines while addressing incident support requests		✓
Administer Client login IDs and reset passwords for Provider ServiceNow data access		✓
Administer Provider login IDs and reset passwords for Provider ServiceNow data access if authorized.		✓
Maintain call-out procedures for Client	✓	
Maintain call-out procedures for Provider		✓
Adhere to established call-out procedures	✓	✓
Record all tickets in Provider ServiceNow solution for all reported incidents, service requests, change requests and problem tickets		✓

System Change Management

Responsibility Description	Client	Provider
Change Management		
Utilize Change Management processes as defined by Provider Process Manual		✓
Receive, process and report change control requests		✓
Conduct Provider internal change control meetings to ensure integrity and quality		✓
Conduct periodic status meetings where Client is in attendance within which change control activities and associated outage windows are reviewed		✓
Participate within periodic Account Management status meetings and review impending change control activity	✓	
Conduct walk-through review of all proposed change control activities		✓
Coordinate Change Management Activities with the Client		✓
Approve, prioritize, and schedule Provider' change control requests	✓	
Conduct post-implementation review meetings as necessary		✓
Provide input and feedback as a result of participating in post-implementation review meetings	✓	
Review and implement mutually agreed recommendations resulting from post-implementation review meetings		✓

Implement client side required measures as recorded and agreed upon during post-implementation review meetings	✓	
System Changes		

Responsibility Description	Client	Provider
Initiate and record change requests		✓
Develop, document, and maintain implementation plans		✓
Estimate time and costs for changes (as applicable)		✓
Review and evaluate estimate upon completion		✓
Write cost justification (as applicable)		✓
Present costs and review need and expense with Client (as applicable)		✓
Approve costs as presented by Provider (as applicable)	✓	
Ensure that change meets Client's prescribed change requirements		✓
Provide input and feedback that Provider' change management processes are meeting Client's prescribed change requirements	✓	
Notify Client of change via documenting the implementation procedure		✓
Coordinate change through the change control process		✓
Negotiate outage window requirements and resources necessary for testing any given change control	✓	
Approve and prioritize order of client's own change control requests	✓	
Provide input regarding a change control allowing Client to provide approval		✓
Provide post-change validation	✓	
Emergency Changes		
Convey the implementation process associated with any given system emergency change requests that impact the Client environment		✓
Approve all system emergency change requests that impact the Client environment	✓	
Implement emergency change in accordance with the established emergency change control procedures		✓
Provide updates to processing procedures for production control impacted by emergency change control implementation	✓	
Provide post-change validation	✓	
Quality Assurance		
Conduct non-prod testing regarding application platform and environment changes and enhancements		✓
Perform procedure audits per mutually agreed upon schedule		✓
Execute non-prod back out procedures associated with change as necessary as a result of a failure during testing		✓
Confirm non-prod application platform and environment testing on system and/or database changes and approve/reject change as necessary within documented specifications	✓	✓
Coordinate user acceptance testing for all changes	✓	
Develop and document back out, back up, and restoration procedures prior to production implementation as part of the change control process		✓
Review and approve documented production back out, back up, and restoration procedures prior to implementation	✓	
Implement change into targeted environment(s) – test, development, quality assurance, production, etc.)		✓
Update ServiceNow Change Request ticket status		✓
Provide post-change validation	✓	
Additional Reporting and Documentation		
Develop, document, and maintain systems change management acceptance specifications		✓

Approve change management acceptance specifications	✓	
Maintain/update Provider' change management process procedures		✓

Incident Management

Responsibility Description	Client	Provider
Utilize Incident Management processes as defined by Provider Process Manual		✓
Provider Operations Center records, logs, prioritizes, assigns severity, and monitors progress.		✓
Maintain incident log, track, and manage timely resolution of open incidents for those issues assigned to Provider		✓
Notify Client analyst or Client Help Desk of the on-going status and final resolution		✓
Pursue successful resolution of Provider assigned incidents		✓
Validate successful resolution of resolved Provider assigned incidents	✓	
Escalate unresolved incidents that exceed established timeframes to appropriate Client and Provider representative(s) as necessary		✓
Close Incident Ticket upon acceptable incident resolution or workaround as verified by Client, providing sufficient detail of incident for later analysis of trends		✓
Document, publish, and keep current procedure for proper Incident escalation within Provider		✓
Document, publish, and keep current procedure for proper incident escalation within Client organization	✓	
Report on metrics of incidents assigned to Provider at account management meetings or as required		✓
Complete Root Cause Analysis (RCA), document, and review high-impact (SEV1, P1) incidents to identify preventative measures, assess risk, and bring to closure		✓
Document RCA input and feedback on reviews of high-impact incidents identifying preventative measures and assessing risk bringing items to closure as appropriate	✓	
Conduct RCA for high-impact incidents or upon Client request		✓
Document input and feedback as a result of receiving and reviewing PIR documentation	✓	
Approve or escalate Provider' recommendations/findings contained within PIR documentation within Client organization	✓	
Implement RCA recommendations/measures as requested/assigned for respective areas of service responsibility within the scope of services		✓
Implement RCA recommendations/measures as agreed upon that require Client engagement resulting from RCA review process	✓	

EXHIBIT E
SELLER GLOSSARY OF DEFINED TERMS

Managed Services – The in-scope managed services Provider is providing per this SOW.

Incident - An unplanned interruption to an IT service or reduction in the quality of an IT service. Application or a function is not performing per standard operating specifications.

Service Request - A request for information, action or advice.

Incident Management – The mission of the Incident Management process is to resolve incident support requests in a timely prioritized fashion.

Service Request Management – The mission of the Service Request management process is to address non-incident type of requests in a prioritized fashion.

Change Management – The mission of the Change Management process is to successfully manage the changes being applied to systems, leading to no further incidents or issues as a result of the changes being applied.

Problem Management – The mission of the Problem Management is to reactively address repeating incidents with goal to prevent them from reoccurring; or to identify improvement opportunities to prevent incidents from occurring in the first place.

Monitoring - The mission of Monitoring is to observe a situation to detect changes or failures that happen over time.

Event Management – The mission of Event Management is to action on events and alerts that occur in the IT environment. Monitoring creates alerts based on predefined criteria. It allows for normal operation and escalates exception conditions.

Defect – Solution is not functioning per design specifications.

New feature or enhancement – Additional functionality, or changes to existing functionality are desired.

Monitoring Tools – A set of tools that monitor key performance indicators on the applications platform and environment, producing events and alerts.

SLA – Service Level Agreement. Service Level Agreements have a financial penalty if missed.

SLG – Service Level Goal. Service Level Goals do not have a financial penalty if missed.

OLG – Operating Level Goal. Operating Level Goals do not have a financial penalty if missed.

OLA – Operating Level Agreement. Operating Level Agreements do not have a financial penalty if missed.

KPI - Key Performance Indicator that may or may not have a financial penalty if missed. The SLAs define items that qualify for a financial penalty if missed. SLG, OLG and OLA do not have financial penalties if missed.

N/A - Not Applicable. Not in use. Not available. Not in services scope.

EXHIBIT E

Extended End Of Life Support

Extended End of Life Support with Commercially Reasonable Effort Support
After a component is partially or fully designated as "end of life," sometimes referred to as "end of support" by a manufacturer, it is no longer sold, manufactured, improved, repaired, maintained, or supported by the manufacturer. As a result, Service Provider cannot provide support on devices designated by the manufacturer as end of life or end of support ("End of Life" or "EOL").

In the interest of offering Client a stable and reliable managed environment, Service Provider recommends that Client maintains a valid hardware and/or software support contract with a vendor. Additionally, Client's firmware, operating system instances, and associated OEM products benefit by being maintained at a vendor supported version/release level. Supported firmware versions are important for the stability of the hardware and to mitigate security vulnerabilities. Service Provider requires validation that vendor maintenance contracts exist for all supported hardware and software. Warranty contracts handle hardware replacement, access to software for upgrades, and a high-level escalation point for problem resolution and bug identification. Maintaining an active warranty contract better protects hardware assets, provides the appropriate resources for critical situations, and helps provide the best possible Client experience.

Extended EOL – Support Included: This covers monitoring services, which may be limited to up/down (i.e., heartbeat monitoring), and limited support for incident management only as outlined below. Client accepts the following risk and terms for devices moved to Extended EOL level support.

Commercially Reasonable Effort Support: Service Provider will attempt to troubleshoot and resolve the issues during regular during business hours by using Service Provider's knowledge and expertise of the product and environment, previously generated vendor knowledge base, and other online and generally available public resources.

Service Provider understands certain business situations may require an exception to these requirements. In the event a Client cannot or chooses not to maintain valid hardware/software support/maintenance/warranty contracts with a vendor and/or has EOL devices, the following risks, limitations and assumptions are necessary:

- Vulnerabilities Due to Patching Limitations
  No new security patches, bug fixes, signature updates, or software updates are available from the manufacturer for Service Provider to apply, leaving Client's components vulnerable. This could result in security exploits and breaches, data loss associated with security events, possible instability due to bugs from non-compatibility of hardware/software or sub-optimal hardware/software performance.
- Removal of Service Level Agreement (SLA) – Availability Management
  - Service Provider cannot provide SLAs on devices designated as End of Life since patches and troubleshooting assistance is no longer available from the manufacturer.
  - Service Provider will not be bound to the Unavailability Credit. If Service Provider is unable to meet the Availability Service Level Agreement due to delays caused by out-of-date firmware, operating system instances, and associated OEM products, Service Provider will not be bound to provide credit for impacted components.
- Limited Troubleshooting
  The Service Provider will no longer be able to engage the manufacturer for support on troubleshooting complex issues. Automation and/or monitoring software may cease to function entirely, have limited function, or may function improperly. There are no guarantees that software packages and tools from the OEM or Service Provider will continue to perform their intended function on non-supported versions.
  - Possibility of long-term or permanent outages of software and hardware:
    There is a possibility of long-term or permanent outages of software or hardware. If hourly support is required from the vendor to resolve an issue, the costs would be passed on to and paid by the Client.
  - Inability to Recover
    If Client's device/software experiences a failure, Service Provider will attempt, but may not be able recover the device configuration, logs, and/or data, restore function or replace the device/software. Client accepts these risks for End of Life devices.
- Limited Reporting

Device release/versions that are not currently supported by performance and monitoring tools are excluded from any contractual reporting.

By signing this agreement, Client understands and acknowledges the following conditions:

- Client acknowledges they are operating in an environment where certain hardware and/or software are out of support and accepts the risks and terms for devices moved to Extended EOL Level Support or Commercial Reasonable Effort Support.
- Client agrees to not hold Service Provider liable should issues arise due to not following Service Provider recommendations.
- Service pricing will be evaluated and potentially updated on a case-by-case basis.
- Service Provider will provide up to 10 hours of engineering support to help resolve individual incidents with Extended EOL level support. Additional support will be provided, if approved by the Client, at the Service Provider's then current Time and Materials (T&M) rates.
  - T&M will be charged to upgrade the firmware and to recover from security breaches should they arise.
- Variability of costs if hourly support is required from vendor to resolve issue.
  - Many vendors only support unmaintained equipment on an hourly basis and during regular business hours (typically M-F 8:00 AM – 5:00 PM) only.
- Service Provider will determine when Commercial Reasonable Effort Support stops and hourly fee-based support from the vendor is necessary. Service Provider will communicate to Client when hourly fee-based support will go into effect. Client is responsible for these vendor costs if they provide Service Provider the request and/or direction to move forward with billable support.
- Service Provider will not use entitlements from a supported system installed at the same location for the acquisition of support or updates on the non-supported environment.
- Client agrees to upgrade as follows:
  - Firmware version upgraded to a vendor supported version within 12 months of signature
  - Replace hardware/software not under maintenance/warranty contracts within 6 months of signature.
  - Make best efforts to upgrade managed devices that are designated as End of Life by the manufacturer within 6 months of the manufacturer's End of Life date. Service Provider reserves the right to discontinue Extended EOL level support following this 6-month period.
- Client agrees to carry, in place of a warranty contract, an inventory of spare equipment that can be used in the event of a hardware failure. Service Provider will comply with this alternative hardware replacement program and will work fully with Client in the event of a hardware failure.
- Client agrees to provide remote hands in the event of a hardware failure. These remote hands are expected to install, rack, and cable the replacement hardware.