Microsoft Enterprise Services Work Order

Work Order Number *(Microsoft Affiliate to complete)*	GVS02506-1011105-1011105

This Work Order consists of the terms and conditions below, and the provisions of the Microsoft Master Services Agreement reference U7752567, effective as of 2/11/2022 (the "Agreement"), the provisions of the Description of Services applicable to the Professional Services identified in this Work Order, and any attachments or exhibits referenced in this Work Order, all of which are incorporated herein by this reference. In this Work Order "Customer," "you," or "your" means the undersigned customer or its affiliate and "Microsoft", "we," "us," or "our" means the undersigned Microsoft affiliate.

By signing below the parties acknowledge and agree to be bound to the terms of this Work Order, the Agreement and all other provisions incorporated in them. This Work Order is effective as of the date that Microsoft signs this Work Order. Regardless of any terms and conditions contained in a purchase order, if any, the terms of this Work Order apply.

Customer
Name of Customer (please print) **County Of Dekalb**
Signature
Name of person signing (please print)
Title of person signing (please print)
Signature date
Name of Customer or its Affiliate that executed the Agreement (if different from Customer above)

Microsoft Affiliate
Name **Microsoft Corporation**
Signature Nick Sabo
Name of person signing (please print) Nick Sabo
Title of person signing (please print) Unified Specialist
Signature date (effective date) 1/23/2025

Does Customer issue or require a Customer purchase order for the payment of Microsoft Services?
[X] **Yes or** [ ] **No**

If "No" is selected above, Customer represents and warrants that it does not require purchase order(s) be submitted to Microsoft for payment of the Microsoft Services Fees listed herein. Customer will not withhold payment of Microsoft's invoice due to the absence of a purchase order reference.

If no purchase order is required, Customer must complete "Customer invoice information" below and ensure it is accurate or revised in a timely manner. Further, the below "Customer invoice information" must be completed prior to: (a) Customer signing this Work Order; and (b) Microsoft invoicing Customer.

Customer invoice information		
Name of Customer County Of Dekalb	Contact Name (Receives invoices under this Work Order) Dekalb County Finance Department.	
Street Address 1300 Commerce Dr	Contact E-Mail Address gwskelton@dekalbcountyga.gov	
City Decatur	State/Province Georgia	Phone
Country United States	Postal Code 30030-3222	Fax

Support Services and Fees

Term.

Microsoft Enterprise Support Services will commence on 6/1/2025 (the "Support Commencement Date") and will expire on 5/31/2028 (the "Support Expiration Date").

Description of Services.

Please refer to the current Unified Support Services Description ("USSD") which will be incorporated by reference and is published by Microsoft from time to time at www.microsoft.com/unified-support-services-description. Microsoft may update the support services you purchase under this agreement from time to time, provided that the level of support services you purchase will not materially decrease during the current Term.

Services by Support Location:

Yr1-Unified Enterprise Support - 2025-26 USA - SLG - Enterprise East 6/1/2025 - 5/31/2026		
Quantity	Service	Service Type
Included	Enterprise Online Support Portal	Administrative
Included	Enterprise Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise Reactive Support Management	Service Delivery Management

Included	Enterprise Service Delivery Management	Service Delivery Management
Included	Enterprise Webcasts As-Needed	Webcast
Included	Reactive Enabled Contacts	Problem Resolution Support
Included	Enterprise Advisory Support Hours As-needed	Advisory Services
Included	Enterprise Azure Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise On-demand Assessment	On-Demand Assessment
Included	Enterprise On-Demand Assessment - Setup and Config Service As-needed	On-Demand Assessment Remote
Included	Enterprise On-Demand Education	On-Demand Education

Yr1-Unified Proactive Services Add on | Unified Proactive Svcs Enterprise Security - 2025-26 USA - SLG - Enterprise East 6/1/2025 - 5/31/2026		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
100 ea	Proactive Credits	Proactive Credits

Yr1-Enhanced Designated Engineering | M365 - 2025-26 USA - SLG - Enterprise East 6/1/2025 - 5/31/2026		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
1,200 hr	Enhanced Designated Engineering Microsoft 365	Designated Support Engineering

Yr1-Enhanced Designated Engineering | Azure IaaS - 2025-26 USA - SLG - Enterprise East 6/1/2025 - 5/31/2026		
Quantity	Service	Service Type
400 hr	Enhanced Designated Engineering Azure IaaS	Designated Support Engineering
Included	Service Delivery Management Extended	Service Delivery Management

Yr1-Enhanced Security | Cybersecurity Incident Response - 2025-26 USA - SLG - Enterprise East 6/1/2025 - 5/31/2026		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
150 hr	Cybersecurity Incident Response Service	Security Services

Yr2-Unified Enterprise Support - 2026-27 USA - SLG - Enterprise East 6/1/2026 - 5/31/2027		
Quantity	Service	Service Type
Included	Enterprise Online Support Portal	Administrative
Included	Enterprise Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise Reactive Support Management	Service Delivery Management
Included	Enterprise Service Delivery Management	Service Delivery Management
Included	Enterprise Webcasts As-Needed	Webcast
Included	Reactive Enabled Contacts	Problem Resolution Support
Included	Enterprise Advisory Support Hours As-needed	Advisory Services

Included	Enterprise Azure Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise On-demand Assessment	On-Demand Assessment
Included	Enterprise On-Demand Assessment - Setup and Config Service As-needed	On-Demand Assessment Remote
Included	Enterprise On-Demand Education	On-Demand Education

Yr2-Unified Proactive Services Add on | Unified Proactive Svcs Enterprise Security - 2026-27 USA - SLG - Enterprise East 6/1/2026 - 5/31/2027		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
100 ea	Proactive Credits	Proactive Credits

Yr2-Enhanced Designated Engineering | M365 - 2026-27 USA - SLG - Enterprise East 6/1/2026 - 5/31/2027		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
1,200 hr	Enhanced Designated Engineering Microsoft 365	Designated Support Engineering

Yr2-Enhanced Designated Engineering | Azure IaaS - 2026-27 USA - SLG - Enterprise East 6/1/2026 - 5/31/2027		
Quantity	Service	Service Type
400 hr	Enhanced Designated Engineering Azure IaaS	Designated Support Engineering
Included	Service Delivery Management Extended	Service Delivery Management

Yr2-Enhanced Security | Cybersecurity Incident Response - 2026-27 USA - SLG - Enterprise East 6/1/2026 - 5/31/2027		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
150 hr	Cybersecurity Incident Response Service	Security Services

Yr3-Unified Enterprise Support - 2027-28 USA - SLG - Enterprise East 6/1/2027 - 5/31/2028		
Quantity	Service	Service Type
Included	Enterprise Online Support Portal	Administrative
Included	Enterprise Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise Reactive Support Management	Service Delivery Management
Included	Enterprise Service Delivery Management	Service Delivery Management
Included	Enterprise Webcasts As-Needed	Webcast
Included	Reactive Enabled Contacts	Problem Resolution Support
Included	Enterprise Advisory Support Hours As-needed	Advisory Services
Included	Enterprise Azure Problem Resolution Hours As-needed	Problem Resolution Support
Included	Enterprise On-demand Assessment	On-Demand Assessment
Included	Enterprise On-Demand Assessment - Setup and Config Service As-needed	On-Demand Assessment Remote
Included	Enterprise On-Demand Education	On-Demand Education

Yr3-Unified Proactive Services Add on | Unified Proactive Svcs Enterprise Security - 2027-28 USA - SLG - Enterprise East 6/1/2027 - 5/31/2028		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
100 ea	Proactive Credits	Proactive Credits

Yr3-Enhanced Designated Engineering | M365 - 2027-28 USA - SLG - Enterprise East 6/1/2027 - 5/31/2028		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
1,200 hr	Enhanced Designated Engineering Microsoft 365	Designated Support Engineering

Yr3-Enhanced Designated Engineering | Azure IaaS - 2027-28 USA - SLG - Enterprise East 6/1/2027 - 5/31/2028		
Quantity	Service	Service Type
400 hr	Enhanced Designated Engineering Azure IaaS	Designated Support Engineering
Included	Service Delivery Management Extended	Service Delivery Management

Yr3-Enhanced Security | Cybersecurity Incident Response - 2027-28 USA - SLG - Enterprise East 6/1/2027 - 5/31/2028		
Quantity	Service	Service Type
Included	Service Delivery Management Extended	Service Delivery Management
150 hr	Cybersecurity Incident Response Service	Security Services

Support Services Fees.

The items listed in the table above represent the services that Customer has purchased for use during the term of this Work Order, and applicable fees are shown in the table below. Microsoft Support Services are non-refundable and prepaid at year one and subsequent anniversaries of the Support Commencement Date. Before Microsoft commences provision of Microsoft Support Services, Microsoft must receive a signed copy of this Work Order and Customer's payment, purchase order or, if applicable, completed Customer invoice information above. Microsoft will invoice Customer, and Customer agrees to pay Microsoft within 30 calendar days of the date of Microsoft invoice. Please note that failure of payment to Microsoft may result in service suspension. Microsoft reserves the right to adjust Microsoft fees in connection with implementing any changes requested by Customer to the Microsoft Support Services ordered herein. Any modified fees will be documented in an amendment.

Support Services Fee Summary	**Year 1 – 06-2025-05-31-2026 (USD)**	**Year 2 - 06-2026-05-31-2027(USD)**	**Year 2 - 06-2027-05-31-2028 (USD)**	**Total (USD)**
Appraised Product Spend	$ 8,710,184.00	$ 8,710,184.00	$ 8,710,184.00	$26,130,552.00
Unified Base Ent	$648,257.79	$648,257.79	$648,257.79	$1,944,773.37
Sub-Total: Microsoft Unified	**$648,257.56**	**$648,257.56**	**$648,257.56**	**$1,G44,772.68**
CybersecurityEnhancedSolutions	$94,425.00	$94,425.00	$94,425.00	$283,275.00
EDE Azure IaaS	$153,065.00	$153,065.00	$153,065.00	$459,195.00
EDE M365	$459,490.00	$459,490.00	$459,490.00	$1,378,470.00
Pro Svs Ent AddOn Sec	$13,245.00	$13,245.00	$13,245.00	$39,735.00
Add-Ons	**$720,225.00**	**$720,225.00**	**$720,225.00**	**2,160,675.00**
Flex Allowance	($129,651.56)	($129,651.56)	($129,651.56)	($388,954.68)
Subtotal Add-Ons	**$5G0,573.44**	**$5G0,573.44**	**$5G0,573.44**	**$1,771,720.32**
Total Fees (excluding taxes)	**$1,238,831.00**	**$1,238,831.00**	**$1,238,831.00**	**$3,716,4G3.00**

*The Microsoft Unified fees described above are based on a tiered rate structure along with the total value each year for Customer's validly licensed, commercially released and generally available Microsoft products, and cloud services subscriptions as identified in Appendix A of this Work Order (collectively, the "Appraised Product Spend") to calculate Customer's Microsoft Unified fees for the 3 Years Support Term.

Prior to each contract anniversary of the Support Commencement Date, Customer's Appraised Product Spend will be re-calculated for the upcoming contract year. If Customer's product spend increases over the previous 12 months ("Actual Product Spend") by more than five percent (5%) above the Appraised Product Spend shown for that year in the Support Services Fee Summary table above, Microsoft will recalculate the associated Microsoft Unified fees for the upcoming contract year. The recalculated Microsoft Unified fees will be based on the Actual Product Spend and the Unified rates listed in the Rate Table below. Microsoft will invoice the customer for the difference between the re-calculated price and the original scheduled Microsoft Unified fees sub-total from the Support Services Fee Summary table above. Customer agrees to pay Microsoft such additional amounts within 30 calendar days of the date of Microsoft's invoice. Please note that failure of payment to Microsoft may result in service suspension. Enterprise Customer may receive additional Flex Allowance which may be applied towards new proactive services, enhanced services and solutions services, and/or custom proactive services. Should Customer fail to allocate the Flex Allowance prior to the contract anniversary, Microsoft may apply the additional Flex Allowance towards new proactive credits.

Microsoft Unified – Rate Table			
Enterprise package	**Server**	**User**	**Azure**
Year 2 Discounted Rate %	10%	6.3%	9.38%
Year 3 Discounted Rate %	10%	6.3%	9.38%

Cybersecurity Incident Response Services Fees.

The Cybersecurity Incident Response Services hours listed in the table below are the services that Customer agrees to pay up front for use during the term of the Cybersecurity Incident Response Services. Accordingly, Customer agrees to pay up front in full the Total Estimated Fees shown in the table below for the Cybersecurity Incident Response Services. All fees paid up front are non-refundable. Any Cybersecurity Incident Response Services hours not consumed prior to the Cybersecurity Incident Response Services Expiration Date will be forfeited. The Total Estimated Fees do not include fees for Products. Customer will pay Microsoft within 30 calendar days of the date of Microsoft invoice.

Cybersecurity Incident Response Services Fees will not exceed the Total Estimated Fees indicated in the table above without prior approval from Customer and a mutually acceptable amendment to this Work Order. In the event that such approval must be sought, but is not provided, notwithstanding anything to the contrary, Customer acknowledges and agrees that Microsoft has no further obligation to continue providing Cybersecurity Incident Response Services.

Billing Schedule	Billing Date (M/d/yyyy)	Fee USD
Y1-Payment	6/1/2025	$1,238,831.00
Y2-Payment	6/1/2026	$1,238,831.00
Y3-Payment	6/1/2027	$1,238,831.00
Total Fees (excluding taxes)		**$3,716,493.00**

Support for Microsoft Products

Microsoft will provide support for Customer's licensed, commercially released, and generally available Microsoft products, and cloud services subscriptions purchased by Customer or Customer's Affiliate: i) under the licensing enrollments and agreements, as indicated in Appendix A; and ii) during the Term of this Work Order. Such products and subscriptions exclude those purchased by any party that is not Customer's Affiliate as of the Support Commencement Date.

Unforeseen Circumstances. In the event of unforeseen circumstances resulting from causes beyond Microsoft's commercially reasonable control, Microsoft will not be responsible for any delay or inability to perform Cybersecurity Incident Response Services.

Public Statements. Customer is not permitted to make any public statements identifying or regarding Microsoft, its Affiliates, or its contractors/subcontractors in relation to the Event or the services, findings, Services Deliverables, or other information provided under this Work Order without its express prior written consent.

Customer Named Contact(s).

Any changes to the named contacts should be submitted to Microsoft Contact.

Name of Customer Support Service Administrator JB Puckett		
Street Address 1300 Commerce Dr		Contact E-Mail Address jbpuckett@dekalbcountyga.gov
City Decatur	State/Province Georgia	Phone 404-637-4134
Country United States	Postal Code 30030-3222	Fax

Use, ownership, restrictions and rights.

Products.

"Product" means all products identified in the Product Terms, such as all Software, Online Services and other web-based services, including pre-release or beta versions. Product availability may vary by region. "Product Terms" means the information about Microsoft Products and Professional Services available through volume licensing. The Product Terms are published on the Volume Licensing Site and is updated from time to time. "Volume Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.

All products and related solutions provided under this Work Order will be licensed according to the terms of the license agreement packaged with or otherwise applicable to such product. Customer is responsible for paying any licensing fees associated with Products.

Fixes.

"Fixes" means Product fixes, modifications, enhancements, or their derivatives, that Microsoft either releases generally (such as service packs), or that Microsoft provides to Customer when performing Professional Services (all support, planning, consulting and other professional services or advice, including any resulting deliverables provided to Customer under this Work Order, to address a specific issue. "Professional Services" means Product support services and Microsoft consulting services provided to Customer under this Work Order. "Professional Services" or "services" does not include Online Services, unless specifically noted.

Fixes are licensed according to the license terms applicable to the Product to which those Fixes relate. If the Fixes are not provided for a specific Product, any other use terms Microsoft provides with the Fixes will apply.

Pre-existing Work.

"Pre-existing Work" means any computer code or other written materials developed or otherwise obtained independent of this Work Order.

All rights in Pre-existing Work shall remain the sole property of the party providing the Pre-existing Work. Each party may use, reproduce and modify the other party's Pre-existing Work only as needed to perform obligations related to Professional Services.

Services Deliverables.

"Services Deliverables" means any computer code or materials, other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services. Upon payment in full for the Professional Services, Microsoft grants Customer a non-exclusive, non-transferable perpetual, fully paid-up license to reproduce, use and modify the Services Deliverable, solely in the form delivered to Customer and solely for Customer's internal business purposes, subject to the terms and conditions of this Work Order.

Non-Microsoft software and technology.

Customer is solely responsible for any non-Microsoft software or technology that it installs or uses with the Products, Fixes, or Services Deliverables.

Affiliates' rights

"Affiliate" means any legal entity that controls, is controlled by, or that is under common control with a party. "Control" means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

Customer may sublicense the rights contained in this section relating to Services Deliverables to its Affiliates, but Customer's Affiliates may not sublicense these rights and Customer's Affiliates' use must be consistent with the license terms contained in this Work Order.

Restrictions on use.

Customer must not (and is not licensed to) (1) reverse engineer, decompile or disassemble any Product, Fix, or Services Deliverable; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (3) work around any technical limitations in a Product, Fix or Services Deliverable or restrictions in Product documentation. Except as expressly permitted in this Work Order or Product documentation, Customer must not (and is not licensed to) (1) separate and run parts of a Product or Fix on more than one device, upgrade or downgrade parts of a Product or Fix at different times,

or transfer parts of a Product or Fix separately; or (2) distribute, sublicense, rent, lease, lend any Products, Fixes, or Services Deliverables, in whole or in part, or use them to offer hosting services to a third party.

Reservation of rights.

Products, Fixes, and Services Deliverables are protected by copyright and other intellectual property rights laws and international treaties. Microsoft reserves all rights not expressly granted in this agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use Software on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

Microsoft Professional Services Data Protection Addendum and Confidentiality.

"Professional Services Data" means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

The data protection terms applying to Professional Services in effect on the effective date of this Work Order and available at https://aka.ms/eswodpa are incorporated herein by this reference.

For liability arising out of either party's confidentiality obligations relating to Professional Services Data provided under this Work Order, each party's maximum, aggregate liability to the other is limited to direct damages finally awarded in an amount not to exceed the amounts Customer paid for the applicable Professional Services under this Work Order.

Attachments

- Couty of Dekalb CybersecurityIncidentResponseExhibitv1.0

Microsoft Contact

Customer contact for questions and notices about this Work Order.

Microsoft Contact Name Nick Sabo	
Phone	Contact E-Mail Address nicksabo@microsoft.com

Appendix A

As of the Support Commencement Date, below is a list of your declared licensing enrollments and agreements for which Microsoft will provide support services as defined within this Work Order.

Customer Name	Licensing Program	Licensing Enrollment/Agreement Number/Billing Account ID
DEKALB COUNTY, GEORGIA	Enterprise 6	6533015
CLERK OF SUPERIOR COURT	MCA	2a6f2eed-1c16-417d-ac24-a44bef7ac76a_2019-05-31
DEKALB COUNTY, GEORGIA	Enterprise 6	82074311
DEKALB COUNTY, GEORGIA-6533015-DEKALB CO AZURE GOV	Enterprise 6	9086545

Microsoft Support Services Exhibit

Cybersecurity Incident Response Services

Enterprise Services Work Order	**GVS02506-1011105-1011105**

This Exhibit is made pursuant to the Microsoft Enterprise Services Work Order identified above ("Work Order"). The terms of the Unified Support Services Description ("USSD") and Work Order are incorporated herein by this reference. Any terms not otherwise defined herein will assume the meanings set forth in the USSD and Work Order.

The term of the Cybersecurity Incident Response Services will commence on **06/01/2025** ("Cybersecurity Incident Response Services Start Date") and will expire on **05/31/2028** ("Cybersecurity Incident Response Services Expiration Date")

Cybersecurity Services Overview.

Customer is entitled to the below specialized cybersecurity-related assistance with the purchase of Microsoft Cybersecurity Incident Response (Cybersecurity Services').

Detailed Service Description.

Requests should be initiated through a support case, as indicated in the USSD. Please note that standard expected response times apply. Support cases will be triaged to specialized teams for additional support, if necessary.

Cybersecurity Services will be provided to you by a team of Microsoft support resources that may include:

- Your Unified Support Customer Support Account Manager ("CSAM") ;
- A team of Microsoft engineers ("Engineers") from the Detection and Response Team (DART) with deep knowledge of cybersecurity Incident Response
- Microsoft Security Cloud Solution Architects (CSAs) with specialized skills to augment the Detection and Response Team (DART) engineers.

How to Engage for a Cybersecurity Incident:

- Open a reactive support case, as outlined in the USSD, noting a potential security incident. Initial investigation will be performed and DART will be engaged when deeper investigation and/or containment measures is warranted.
- Standard expected response times apply for all reactive support cases.
- All proactive engagement requests will be initiated through the Customer's Customer Success Account Manager (CSAM).

How to Engage for pre-incident Services:

- Contact your CSAM to scope and schedule pre-incident Services.

Incident Response Services:

1. **Services Within Scope**

Areas within scope	Assumptions

Pre-Incident Services
Customer may use available Cybersecurity Incident Response hours for pre-incident Services.
• Types of Services Within Scope
  ○ Cybersecurity Incident Response service onboarding
  ○ Compromise assessments
  ▪ Cybersecurity Zero Trust architecture and resiliency risk assessments
  ○ Threat intelligence briefings
  ○ Incident Response Plan (MIRP) best practices review and preparedness feedback
	• specific scope and hours estimates customized per delivery
	• Standard staffing lead times apply
	• Services out of Scope: Non-Security related engagements

On-Premises System Investigation:
• Investigation of Windows environments, including:
  ○ Workstations
  ○ Member servers
  ○ Domain controllers
• Investigation of Linux environments within the supported distributions/versions.
	• The assessment provides:
	  ○ Threat hunt and forensic analysis of machines of interest.
	  ○ Reverse engineering of suspicious files.
	  ○ Security configuration assessment of Active Directory/Microsoft Entra ID.
	  ○ Analysis /remediation of supported endpoints
	• Linux endpoints may be in scope for cybersecurity Incident Response engagements, but in a limited format. In-scope, non-Windows operating systems may include, but are not limited to:
	  ○ Red Hat—Red Hat Enterprise Linux (RHEL), Fedora, CentOS, AlmaLinux, and Oracle Linux.
	  ○ Debian—Debian, Ubuntu, Mint OS, and Kali.
	  ○ SUSE—openSUSE, SUSE Linux enterprise desktop (SLED), and SUSE Linux Enterprise Server (SLES).
	Investigation of MacOS systems, where Defender for Endpoint (MDE) can be deployed
	
	Note that compatibility with Microsoft security technologies may be dependent on kernel version. Previous kernel versions may be

Areas within scope	Assumptions
	supported on a commercially reasonable effort basis. Out of scope operating systems include (but are not limited to): ○ Custom Linux kernels ○ BSD
Microsoft Entra ID & O365 Investigation: Microsoft will assist with assessment of Microsoft Entra ID/Office 365 environments, including: • O365 tenant(s) • Microsoft Entra ID (AAD)	Assessment provides: • Investigation of suspected identities and potentially compromised accounts • Investigation of key data points across O365 services • Security components assessment of O365 Architecture • Risk management recommendations to protect O365 services • Custom threat profile of high-risk users
Tactical Recovery & Containment: • Assistance in containing and recovering from a security incident, which includes support for: ○ Restoration and hardening of critical Tier 0 assets, such as Microsoft Entra ID, HyperV, Windows Server Update Services (WSUS), Active Directory Federation Services (AD FS), and Active Directory Certificate Services (AD CS). ○ Hardening of key cloud services related to the protection of attack paths frequently used by Threat Actors in products such as Exchange Online Protection (EOP), Defender for Office 365 (MDO), Microsoft Entra ID and it's associated sub-services. ○ Regain control of the customer's Microsoft identity by disrupting the attacker's activity. This may be achieved through a combination of actions including: close the Command-and-Control (C2) channels, harden identity, endpoints, and servers, isolate and rebuild planning and support or guidance of compromised systems.	

2. Services Out of Scope – Incident Response

Any area not explicitly listed in "Areas Within Scope" is out of scope for this Exhibit. Out of scope areas for this engagement include, but are not limited to, the following:

- Analysis of Networking equipment
- Comprehensive analysis of endpoints running legacy (unsupported) operating systems

- Data migration activities
- Provision of formal training
- Decryption support for encrypted files or hosts
- Investigation, validation, or remediation of individual security alerts or indicators of compromise outside of active incident response engagement
- Constant, or continuous, security monitoring after the engagement has concluded and/or monitoring outside of standard business hours
- Providing decryptors for encrypted systems
- Ransomware negotiation
- Any work that is required to meet evidentiary standards for legal admissibility in a court of law
- Preparation of systems run books, playbooks, or operational manuals
- Project management of individual projects
- Asset discovery and inventory

3. Assumptions

Support services delivered under this Exhibit are based on the following prerequisites and assumptions:

- This Exhibit is considered the baseline scope document outlining Microsoft's responsibilities for assistance.
- This Exhibit is generated based upon currently known information deemed to be accurate and correct.
- All Support Service resources will have the appropriate level of security access and access to relevant data required to complete Project-related efforts.
- All work is delivered during normal business unless otherwise mutually agreed.
- Cybersecurity Incident Response is typically staffed by a shared cybersecurity incident responder r esource pool.
- Only currently supported Microsoft operating systems are guaranteed to be in-scope. Non-supported Microsoft operating systems may be deprecated from analysis at any time.
- Written deliverables are available in English language only.
- Services may be delivered remotely or onsite at customer location based on the agreement of the parties.

Customer will provide:

- Accurate and complete information provided, as needed, including identification of systems of interest, overviews of IT infrastructure/topology, and findings from relevant investigation(s).

- Subject matter specialists and Systems Administrators, as necessary, so that proper access to system may be obtained.

- Timely decisions and approvals by management, as needed.

- Full empowerment for security incident responders to fully perform the forensic investigative processes and procedures it employs as part of its standard protocols, free of encumbrances created by third-parties, such as other incident response vendors. Any failure by Customer, or its representatives or agents, to fully empower Microsoft to perform its work may result in delays of service or inadequate outcomes.

4. Customer System Requirements

- An operational solution to remotely deploy the required tools for the Incident Response engagement (e.g., SCCM, Active Directory GPO, or other).

- Maintain Microsoft Entra ID accounts with Global Administrator permissions, as needed.

- Deployment of specialized analytics tools, indicated and provided by the Microsoft cybersecurity delivery team. Tools required for analysis, may include the following, among a range of potentially required analytics tools:

    - Fennec: Fennec is a Microsoft proprietary tool, which will be provided by Microsoft directly to the Customer when ready to deploy. Fennec is an "agentless", one-time scanning tool that provides an investigative snapshot of scanned machines.

    - Linux Forensic Examination Tool("LIFE"): LIFE is a proprietary tool, which will be provided by Microsoft directly to the Customer when ready to deploy. LIFE gathers a snapshot of information about files, programs, processes, and users on Linux machines throughout their organization to augment the Incident Response investigation.

    - FoX: FoX is a proprietary forensics tool deployed to machines if particular interest or where deeper additional information is required.

    - Arctic : Arctic is a tactical identity forensics tool that enumerates aspects of Active Directory Domain Services to allow for identification of adversary persistence

    - Cosmic: COSMIC is an Azure cloud forensics tool that enumerates aspects of Entra ID to allow for identification of adversary persistence.

    - Microsoft Defender for Endpoint: Microsoft's endpoint detection and response (EDR) solution provides continuous monitoring for additional adversary activity. An agent is required for in-scope, non-Windows 10/11 machines.

- Microsoft Defender for Identity: Defender for Identity analyzes authentication traffic on Customer's Domain Controllers to identify suspicious activity and identity-based attacks. Solution requires an agent to be deployed to each Domain Controller, Active Directory Certificate Services (ADCS) and Active Directory Federation services (ADFS) where applicable.

5. Access required for analysis:

- Global Administrator access in Microsoft Entra ID is required for successful completion of the engagement.

- Microsoft may leverage access into your Azure and Office 365 environment to perform analysis and investigation.

Note: Microsoft will notify Customer if additional tools are required based on initial findings and understanding of the specific scenario.

6. Deliverables

Deliverables for Cybersecurity Incident Response engagements may include:

Deliverable	Description
Outbrief Report	an "outbrief" document in Microsoft Powerpoint format, prepared by the delivery team, summarizing key investigative findings, which may include assessment of risk and/or recommendations for remediation
Outbrief Presentation	an outbrief presentation to Customer verbally to communicate the findings described in the outbrief document
Timeline Report	if technically feasible and supporting data exists, a timeline document in Microsoft Excel identifying and documenting the location of relevant supporting data and files analyzed during the course of the engagement
Power BI Dashboard	a Microsoft PowerBI Dashboard showing technical information concerning the findings from the Fennec scanner, except in rare circumstances when it cannot be generated for technical reasons

Deliverables (as defined above) will be delivered within the ten (10) calendar days following the conclusion of the Cybersecurity Incident Response engagement, unless Customer choose not to receive the Deliverables. The Customer's choice not to receive the Deliverables is no fault of Microsoft under any circumstances, and any obligation of Microsoft to deliver said Deliverable(s) expires 10 calendar days after the final day of the engagement, unless otherwise mutually agreed by Microsoft and Customer.

Cybersecurity Incident Response deliverables may provide the following:

- Identity of systems that may be compromised

- Identity of systems that may be vulnerable (e.g., machines missing critical patches and/or antivirus definitions and identification of commonly exploited applications)
- Results of forensic analysis of hosts of interest
- Results of reverse engineering of suspicious files
- Guidance for a customer to take proactive steps to improve their security posture

Cybersecurity Incident Response deliverables do not provide the following:

- Attribution of attacker including the identity, motives or origin
- Chain of custody of evidence (e.g., IOCs)
- Compliance assessment with any standard or framework, e.g., security or privacy standards
- Remediation efforts
- Source code review
- Organizational change management
- Technical and/or architectural IT systems design
- Detailed analysis or risk assessments of existing security controls and how they are implemented

Customers who seek findings pertaining to compliance and regulations should be conducted separately by professional services firms that specialize in audit and assurance. Customers should independently validate whether a Microsoft Cybersecurity Incident is covered by their insurance policy, if applicable.