Microsoft Support Services Exhibit

Cybersecurity Incident Response Services

Enterprise Services Work Order	**UED02601-1029489-1029489**

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.

Customer	**Microsoft Affiliate**
Name of Customer (please print) **Dekalb County School District**	Name **Microsoft Corporation**
Signature	Signature
Name of person signing (please print)	Name of person signing (please print)
Signature date	Signature date

The term of the Cybersecurity Incident Response Services will commence on 01/01/2026("Cybersecurity Incident Response Services Start Date") and will expire on 12/31/2026 ("Cybersecurity Incident Response Services Expiration Date")

1 Overview and scope of coverage

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

1.1 Onboarding

MSCIR services will be provided by a team of Microsoft support resources that may include:

- A Unified Support Customer Support Account Manager ("CSAM").
- Microsoft support engineers with security expertise.

- Microsoft engineers from the Microsoft Incident Response ("MSIR") team with deep knowledge of cybersecurity incident response.
- Microsoft Security Cloud Solution Architects ("CSA"s) with specialized skills to augment the MSIR team.
- Additional Microsoft security experts, at the discretion of the MSIR team.

How to Engage for a Cyber-attack incident:

- Open a reactive support case, as outlined in the USSD, noting a potential security incident. Initial investigation will be performed, and the MSIR team will be engaged when deeper investigation and/or containment measures are warranted.
- Standard expected response times apply for all reactive support cases.

How to Engage for pre-incident MSCIR services:

- Contact the CSAM to scope and schedule pre-incident MSCIR services.

1.2 Incident Response Services

- Services Within Scope

Pre-Incident Services	
Areas within scope	**Description**
• Threat Briefing	Highly specialized Microsoft Security researchers provide tailored threat intelligence advisory services, enhancing defense strategy with customized threat intelligence informed by industry-specific threats.
• Tabletop Enhanced (Premium)	Helps identify potential gaps in incident response plan and improves collective decision-making during incidents. Customer's team will walk through security events, providing evidence to Microsoft engineers who will guide and help evaluate Customer's ability to identify and respond to each scenario. Includes collaborative exercise guiding participants through simulated incident scenarios.
• Proactive Identity Assessment	Helps to protect from targeted attacks by sophisticated adversaries and criminal organizations, offering a thorough evaluation of Control Plane, pinpointing critical security risks and providing actionable recommendations.
• Proactive Identity Hardening	Utilizes automation to deploy Secure Keyboard, including Conditional Access Policies, required Groups, Break Glass Accounts, Intune Policies and AutoPilot. Includes the continued deployment of the

Pre-Incident Services	
Areas within scope	**Description**
	tiering model, onboarding one workload to Tier 1. Optional security assessment of Entra ID, discussions on recommended practices for MDE, MDI and MDC. Also initiates Laps implementation.
• Compromise Assessment	Highly specialized Microsoft resources providing remote analysis, effectively serving as an incident response prior to an actual emergency. Assessment will provide the findings that identify systems that may be compromised or vulnerable, along with recommendations to guide Customer on taking proactive measures to improve security posture.

On-Premises System Investigation	
Areas within scope	**Description**

• 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 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.
	• 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.

1.3 Services Out of Scope – Incident Response

Anything not explicitly listed in "Areas Within Scope/Description" is out of scope for this service, including but 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
- Denial of Service (DoS) attack

2 Assumptions

MSCIR 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 MSCIR 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 hours unless otherwise mutually agreed.
- MSCIR is typically staffed by a shared cybersecurity incident responder resource 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.
- Notwithstanding the USSD, a previously scheduled paid additional service may not be canceled or rescheduled and is non-refundable unless both the Customer and Microsoft mutually agree otherwise in writing.

3 Customer's responsibilities

- Provide accurate and complete information, as needed, including identification of systems of interest, overviews of IT infrastructure/topology, and findings from relevant investigation(s).
- Provide subject matter specialists and systems administrators, as necessary, so that proper access to system(s) may be obtained.
- Provide timely decisions and approvals by management, as needed.

- Grant full empowerment for MSCIR 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 MSCIR engagement (e.g., SCCM, Active Directory GPO, or other).
- Provide Microsoft Entra ID accounts with Global Administrator permissions, as needed.
- Deployment of specialized analytics tools indicated and provided by the MSCIR 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 MSCIR 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 Power BI 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 MSCIR engagement, unless Customer chooses 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 ten (10) calendar days after the final day of the engagement, unless otherwise mutually agreed by Microsoft and Customer.

MSCIR 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

MSCIR 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 cyber-attack incident is covered by their insurance policy, if applicable.

7 Fees

Fees associated with this Exhibit will be detailed in the Work Order.