Statement of Work

28957 – DeKalb County School District- Managed Services

This Statement of Work ("**SOW**") is entered into between Cyderes Group LLC ("**Supplier**") and DeKalb County School District ("**Customer**"). Any changes made by Customer to this SOW not authorized and initialed by Supplier are null and void.

Customer acknowledges that Supplier may use any of its Affiliates to perform certain obligations under this SOW. "Affiliate" shall mean any direct or indirect, current, or future subsidiary of a party, or any other entity controlled by, or under common control with, or which controls such party.

This SOW is subject to and governed by any existing Master Services Agreement or equivalent ("MSA"), which is incorporated herein by reference in its entirety, currently in place by and between Supplier and Customer (or Customer's Affiliate, with all terms and conditions applicable to Customer) that expressly authorizes Customer to purchase the services described hereunder. In the event that such an MSA is not in place, this SOW shall be subject to and governed by the terms included in Appendix below. Any terms and conditions set forth in a purchase order issued by Customer for this SOW that are in addition to or that conflict with the MSA and/or this SOW, shall not apply and are to be considered null and void.

Table of Contents

Statement of Work

28957 – DeKalb County School District- Managed Services

1. Purpose

1.1 Customer has partnered with Supplier to Onboard the In-Scope Managed Technologies (the "Technologies") and provide the In-Scope Managed Services (the "Services") listed in the corresponding sub-sections of **Section 2. Summary**.

1.2 The Services and Technologies will be Onboarded as detailed in **Section 4. Onboarding Service Description**.

1.3 Anything not clearly listed in the Services is considered out of scope.

2. Summary

2.1 Onboarding Services Summary

2.1.1 Enterprise Service Onboarding Structure:

Ready-up	▸ Review the scope of Onboarding Services and In-Scope Managed Services as listed in the SOW. ▸ Establish governance, cadence, reporting, resource, and technical requirements for Onboarding Services.
Kick Off	▸ Draft relevant service architecture artifacts.
Onboard	▸ Configure the technical architecture based on the drafted architecture artifacts. ▸ Build relevant detective and operational content which may include the deployment of logic, creation of Supplier Runbooks, and Tuning.
Transition to Operate	▸ Perform end-to-end system testing, as needed. ▸ Confirm and document that the solution is functioning as expected.

2.2 In-Scope Managed Technologies

2.2.1 The Supplier will deliver the Services leveraging the Technologies listed below. Leveraging any technology not listed below is considered out-of-scope for this SOW.

2.2.2 In-Scope Managed Technologies Details:

Device Type	Manufacturer(s)	In-Scope Notes
SIEM	Microsoft Sentinel	▸ 6,600 Teachers/Knowledge Workers, and 15,000 Total Users ▸ Single tenant ▸ Existing license ▸ The Supplier will leverage the Microsoft Lighthouse solution for management
EDR	Microsoft Defender for endpoint	▸ 30,000 Endpoints ▸ Existing license

2.3 In-Scope Managed Services Summary

2.3.1 Supplier will provide the Services by leveraging the Technologies listed in Section 2.2. Supplier is limited to the coverage of the Technologies as defined in the In-Scope Managed Technologies Details section.

2.3.2 The Service offers 24x7x365 outcomes for detection, investigation, and escalation/containment. All relevant service limits and service levels are articulated in the relevant sections.

2.3.3 In-Scope Managed Services Summary Details:

Service Type	Services
Threat Advisory	▸ Develop threat intelligences ▸ Assess and communicate emerging risks to Customer ▸ Directs threat detection ▸ Manage threat intelligence
Platform Management	▸ Manage the underlying health, availability, and capacity ▸ Perform relevant changes ▸ Manage the ingest and parsing of data sources
Threat Detection	▸ Manage the development of relevant controls
Security Alerting	▸ Identify and investigate security anomalies within the estate ▸ Support Customer in their mitigation by providing security information, advice, and guidance.
Customer Success Services	▸ Manage the Customer portal ▸ Provide Customer Success support

3. Term

SOW Effective Date	The date this SOW is signed and executed. See SOW Acceptance.
SOW Invoicing Dates	Onboarding Services and Year 1 In-Scope Managed Services shall be invoiced in full on the SOW Effective Date. Year 2 and 3 In-Scope Managed Services shall be invoiced in full on the first and second anniversary of the SOW Effective Date, respectively.
Initial Term	The Initial Term of the SOW shall begin upon the SOW Effective Date and end after thirty-six (36) months.
SOW Termination Rights	This SOW cannot be terminated at any time before the end of its Term. Any applicable 3rd Party Products including In-Scope Managed Technologies, shall be subject to the terms of this SOW or a Quote if applicable.

4. Onboarding Services Description

4.1 Onboarding Services Outcomes

4.1.1 Each Onboarding Services Deliverable (the "Deliverables") must be mutually accepted as complete. The Supplier will provide weekly project updates to the Customer tracking each of the Deliverables outlined below by their corresponding reference number.

4.1.1.1 Where a Deliverable is at risk due to the Customer not meeting the required dependencies, the Customer will be informed in the project update.

4.1.1.2 Where the Customer does not meet dependencies for two concurrent reporting periods, the Supplier reserves the right to introduce additional onboarding charges or, where delay relates to telemetry only, commence the effected In-Scope Managed Service leveraging only the telemetry sources available.

4.1.2 The Onboarding Services will begin within a reasonable timeframe from the SOW Acceptance Date via communication from the Supplier. The Onboarding services are anticipated to last up to 8 calendar weeks assuming all dependencies can be mutually accepted, and will be carried out by a qualified and experienced Supplier onboarding team from our Managed Services pool of technical talent.

4.2 Onboarding Managed SIEM – Standard Deliverables

Ref	Phase	Task	Deliverable	Evidence of Completion
D-01	Ready Up	Project Plan	Project plan in Supplier format delivered to Customer. This will include: • Milestone updates • RAID • RASCI • RAG/TLP (Risks)	Delivered timeline
D-02	Ready Up	Prerequisites	Customer to confirm all Onboarding pre-requisites have been successfully delivered. These include: • Network diagram (to validate forwarding requirements) • Assigned resources • Tiered log source list (see Appendix D) • Escalation Procedure Document • Upcoming change restrictions	Customer to confirm delivery of required pre-requisites within 5 business days of request being made
D-03	Kick-Off	Kick off Call	• Project timeline run-through • Schedule meeting cadence • Confirm dependencies (resources, technology) • Confirm key roles	Kick off presentation evidenced, recorded, and associated artifacts provided to Customer

			• In-scope service overview & limitations • Customer expectations	
D-04	Kick-Off	Establish & validate access	Relevant access to In-Scope Managed Technologies confirmed	Supplier confirms all access is established and maintained

D-05	Kick-Off	Architecture & Design	The following artifacts will be delivered leveraging Supplier templates:
			• Service Catalogue
			• Service Delivery Document
			  ○ Data source list
			  ○ Use case list
			  ○ High-Level Design
				Documents embedded in Completion Certificate

D-06	Onboarding	Data acquisition	See Appendix D for in scope Onboarding data sources. The Customer shall select up to 8 data sources for initial Onboarding. Acquisition and parsing of in scope data sources to ensure suitability for detection content	Screenshots evidencing ingestion of relevant telemetry and added to Completion Certificate
D-07	Onboarding	Detection content	Detection content enabled, tested, and deployed into production, including relevant MITRE ATT&CK- alignment	Rules deployed to SIEM technology
D-08	Onboarding	Customer portal	Establish access to the customer portal with relevant dashboards and reports configured for the Customer	Confirmation of client access by client.
D-09	Transition to Operate	Customer enablement	A single, recorded enablement session guiding the Customer through in scope Services and how to interact with the service **Note**: vendor technical training is not in scope	Recording and relevant enablement documentation provided to Customer
D-10	Transition to Operate	System health check	A final system health check confirming the following components acting as expected, including: • forwarding infrastructure • data ingest • deployed security Rules	Completed final 'go live' system health checks as detailed in the Completion Certificate
D-11	Transition to Operate	E2E Event walkthrough	A single security detection Alert in the production system, evidenced to the Customer, confirming all technology interacting as expected.	Recorded Alert walkthrough with evidence added to Completion Certificate

D-12	Transition to Operate	Completion Certificate	Document evidencing all technology, telemetry, and Alerting deployed into production environment. Any Deliverables not complete due to the Customer not meeting required dependencies will be detailed and accepted by the Customer.	Completion Certificate reviewed and approved by Customer stakeholder

4.3 **Onboarding Managed SIEM – Microsoft Sentinel**

Ref	Phase	Task	Deliverable	Evidence of Completion
D-00	Ready Up	Health check & remediation of existing instance	Completed remediation activity of up to 5 days effort and health check report	Health check report provided to Customer. Where remediation requires more than 5 days effort, additional days will be agreed and charged on a time and materials basis
D-01	Ready Up	Gain & activate Microsoft Sentinel license instance	Microsoft Sentinel instance provisioned and accessible	Access gained to platform
D-02	Ready Up	Enable Lighthouse multi-tenancy	Align Customer instance within Lighthouse	Supplier to confirm access via Lighthouse instance
D-03	Ready Up	Deliver config details for any relevant on-premises architecture (as defined by build book)	Requirements sent to Customer	Requirements sent to Customer
D-04	Onboarding	Data parsing	Evidence of data parsing	

4.4 **Onboarding Managed Detection & Response**

Ref	Phase	Task	Deliverable	Evidence of Completion
D-01	Onboarding	Escalation criteria	Building of escalation parameters and integrations (P1-P3)	Documented escalation criteria signed off by Customer and Supplier
D-02	Onboarding	Process documentation	The following artifacts will be completed • Customer handbook • Access management • Supplier processes	Documentation signed off by Customer and Supplier

D-03	Onboarding	Alert integration	Enabling Alert sources to be ingested into the Supplier Platform	Integration between Alerting technology and Supplier Workflow Solution
D-04	Transition to Operate	E2E Test	Alert walkthrough	Test documented within Jira ticket

4.5 **Onboarding Managed EDR – Standard Deliverables**

Ref	Phase	Task	Deliverable	Evidence of Completion
D-01	Ready Up	Identify critical endpoints & OS	Supplier provide recommendations based on industry best practices on agent deployment	Customer approved list
D-02	Ready Up	Health check & remediation of existing instance, if applicable	Report any identified high severity events	Completed health check report
D-03	Onboarding	Access	Login Information for Supplier to access platform	Accessing party login attempt
D-04	Onboarding	Policy	Creation of detection and containment policies aligned with technology best practices	Demonstrate policy configuration
D-05	Onboarding	Alert integration	Enabling Alert sources to be ingested into the Supplier platform	Integration between Alerting technology and Supplier Workflow Solution
D-06	Onboarding	Setup EDR logging to SOC.	Evidence of alignment	Confirmation via platform
D-07	Transition to Operate	E2E Test	Alert walkthrough	Test documented within Jira ticket

5. In-Scope Managed Services Detailed Description

5.1 This section describes the In-Scope Managed Services being provided by the Supplier to the Customer and take precedence in the event of conflict with another section of this SOW.

5.2 Service capacity volumes are listed in the below tables. Should the Customer require additional capacity units beyond those included in the SOW, these may be procured through either a one-off payment to deliver a single point in time requirement, or a change request to increase ongoing capacity.

5.3 **Threat Advisory Services**

Service	Description	Service Capacity/Deliverable
Horizon Scanning	Monitoring for new and adapting adversary behavior, assessing new threats, and prioritizing adversary assessment.	Regular threat briefings

	This service provides clients with regular briefings relating to salient threats and recommendations on mitigating activities	
	Inputs: Threat research, emerging threats, zero-day publications	
Indicator Management	Management of Supplier threat intelligence through collection, processing, analysis, dissemination, and pruning of Supplier threat intelligence feeds to strive for content that is current, relevant, and of high fidelity.	Regularly updated threat intelligence feeds
	Input: Event triage, horizon scanning, reported false positives (pruning), reported true positives (curation)	

5.4 **Platform Management Services**

Service	Description	Service Capacity/Deliverable
Service Monitoring & 1st Line Break/Fix	Identifies, responds to, and fixes deficiencies within the Technologies, including monitoring for platform issues, silent Log Sources, inability to search, and license violations. For any deficiencies or bugs in the Technology itself, the supplier will engage with the Vendor directly to establish root cause and longer-term remediation plans.	Resolved Incidents, Customer escalations or problem tickets raised with Vendor
	Input: Service monitoring Alerts generated into the workflow solution or Customer reports, regular checks, Customer notification	
Patches/Upgrades	Deploying vendor approved and released patches or upgrades to ensure the Technology remains in support, secure, and takes advantage of released features	All Technology components to be in support by the Vendor.
	Input: Customer request, security vulnerability announcement	
Data Engineering	Identifying and implementing the most appropriate mechanism of data collection, parsing, and retention. This may include agent deployment, API inputs, or syslog management. Aligning collected data into the correct format to allow the platform and relevant detection content to be deployed. This may include data abstraction	Appropriately configured & mapped telemetry within the Technologies, with prioritization based on security value that can be derived.

	methods for common detections or aligning data to a normalized set of fields.	Includes 1 new Onboarding per quarter
	Input: Customer request, Customer backlog, Supplier recommendation	

5.5 **Threat Detection Services**

Service	Description	Service Capacity/Deliverable
Detection Content	Identification, creation, testing, and deployment of search logic designed to detect a specific attack scenario or compliance requirement. Examples may include regulation or attack scenarios.	Cyderes detection content updated and reported on quarterly and as needed to monitor for emerging threats.
	Input: Custom requests, regulatory requirements, threat hunting, security Incidents, threat research	
Logic Amendment (Platform)	The Logic Amendment service component includes the amendment of Detection Content at an atomic level to improve alert fidelity. This may include adding to allow/block list or amending thresholds within the search logic. Any rewrite of existing content beyond these parameters will not be considered a Logic Amendment and instead treated as new Detection Content.	Successfully implemented change and updated logic in SIEM
	Input: Customer request, Supplier identified Tuning opportunity	

5.6 **Security Alerting Services**

Service	Description	Service Capacity/Deliverable
Contextual & Intelligence Enrichment	Taking Alerts received into the Supplier SOAR Platform and enriching with relevant and actionable intelligence to improve Alert fidelity and time to escalation. This may include correlation with Cyderes Threat Intelligence and other OSINT enrichment services and internal business context provided by the Customer.	Successfully implemented change and updated logic in Supplier technology
	Input: Customer request, Supplier identified tuning opportunity	
24x7x365 Security Triage	Responding and analyzing identified security Alerts (whether automated or human led), to ensure an appropriate response considering the Alert priority,	Completed ticket investigation resolved as one of the following: escalated to client, Event

	type, asset & user type, and any other relevant information available. Completed triage may include dismissing the Alert as false positive, escalating events to the Customer with a clear investigative story and recommendations for client next steps, taking containment action or recommending the detective content be amended.	dismissed, record valid activity, mitigate activity, escalated to Incident response
	Input: Security Alerts generated into the Supplier workflow solution	
Event Containment	An extension of Event resolution, Supplier will take preauthorized containment/isolation actions on select Customer technology	Confirmation of Event containment
	Input: Event triage	

5.7 **Customer Success Services**

5.7.1 The Customer (including all desired staff) will have access to dashboard reporting through a Customer Portal.

5.7.2 The Services in-scope are managed via a Customer Success Process. Any task or activity listed below is completed during Regular Business Hours (8:30 AM to 5:00 PM in the Customer's local time-zone).

~~5.7.2~~5.7.3 The below listed services will be reviewed Quarterly during a Quarterly Business Review call that will be scheduled by the CSM. Additionally, bi-weekly or monthly calls can be scheduled with the CSM to discuss specific Customer requests, including but not limited to: tuning, filtering, gaps coverage, etc.

Service	Description	Owner
Services Gap Analysis	Identify gaps between purchased deliverables and Customer goals. If applicable, highlight opportunities where other services can support Customer goals.	Supplier
Services Oversight	Review/monitor any active tickets, escalations, Customer e-mails, and milestones.	Supplier
Knowledge Database Management	Recommend and communicate any changes to the documentation stored on the Knowledge Database.	Supplier / Customer
Services & Roadmap Management	• Single and first point of contact for purchased services. • Fully manage services roadmap, highlighting accomplishments, adjustments, next steps, and additions to the roadmap.	Supplier

	• Measure progress of milestones and roadmap delivery dates. Communicate next steps, risks/issues, and questions. • Analyze data outputs from services and business intelligence tools • Collect client feedback and deliver to Supplier services and product teams for improvement.	
Security Recommendations	• Provide recommendation on how to improve services, processes, and/or technologies based on data outputs from services and business intelligence tools • Provide recommendation on how to improve defensive coverage based on telemetry logging.	Supplier

6. Fees

6.1 Fee Summary

SKU	Description	Amount
CYD-MS-ONBOARDING	SIEM Onboarding Services	$45,000.00
Onboarding Services		**$45,000.00**
CYD-MS-PLATFORM-SIEM-Sentinel CYD-MS-PLATFORM-EDR-Defender CYD-MS-MDR	Threat Advisory Services	$678,960.00
	Platform Management Services	
	Threat Detection Services	
	Security Alerting Services	
	Customer Success Services	
Year 1 In-Scope Managed Services		**$678,960.00**
CYD-MS-PLATFORM-SIEM-Sentinel CYD-MS-PLATFORM-EDR-Defender CYD-MS-MDR	Threat Advisory Services	$678,960.00
	Platform Management Services	
	Threat Detection Services	
	Security Alerting Services	
	Customer Success Services	
Year 2 In-Scope Managed Services		**$678,960.00**
CYD-MS-PLATFORM-SIEM-Sentinel CYD-MS-PLATFORM-EDR-Defender CYD-MS-MDR	Threat Advisory Services	$678,960.00
	Platform Management Services	
	Threat Detection Services	
	Security Alerting Services	

	Customer Success Services	
Year 3 In-Scope Managed Services		**$678,960.00**

6.2 **Fee Notes**

6.2.1 Invoicing Schedule is detailed in **Section 3. Term**.

6.2.2 Pricing Terms are listed in Appendix C.

7. Service Assumptions

7.1 **Onboarding**

7.1.1 A kickoff call will be scheduled within a reasonable timeframe of SOW Effective Date and held by the Supplier to review subscription and general services overview.

7.1.2 A weekly cadence call will be scheduled for up to eight (8) weeks to integrate critical data types.

7.1.3 Ad Hoc meetings will be scheduled as needed for technical breakout sessions.

7.1.4 Supplier has published API documentation to implement ticketing integration. Documentation can be found at the following location: docs.cyderes.cloud. The Supplier will provide advice and guidance on integration; however implementation will be a responsibility of the Customer.

7.1.4.1 The case adjustment in the Supplier system will update the case in the Customer system; the field mapping will be done by Supplier (Username, subject, etc.).

7.1.4.2 Supplier will ensure standard field schema. Any fields outside the standard schema requested to be integrated may be subject to additional mutually agreed upon costs if accepted.

7.1.4.3 Supplier will require a service account for authentication to verify the access to the specific API Endpoint.

7.1.5 During and after onboarding Supplier and Customer will discuss what playbooks are required and how to incorporate them into the Automation/ Logic Apps functionality in the Supplier SIEM.

7.2 **Throughout the term**

7.2.1 All Services will be provided from the Supplier's chosen workflow solution which the Customer can access through the Customer portal.

7.2.2 Supplier may require certain administrative access to In-Scope Managed Technologies added throughout the term if owned and/or hosted by the Customer.

7.2.3 Where a new data source is requested where an integration does not exist, delivery is subject to special agreement between the Customer and Supplier.

7.2.4 The Supplier will leverage a Supplier managed federated SSO solution, or approved MSSP access method for access to all In-Scope Managed Technologies.

7.2.5 Supplier will schedule a service review meeting once per month to discuss operational issues held with the Customer.

7.2.6 Supplier will be added as the Claiming Partner of Record (CPOR) for all Microsoft 3665 workloads that may be affected as part of this agreement.

7.2.7 Supplier's Microsoft Partner ID will be added to the relevant Azure subscription in client's Azure environment via Partner Admin Link (PAL) or Digital Partner of Record (DPOR).

7.2.8 The Customer will have a mechanism to send logs from Endpoints to the Supplier, utilizing a relevant forwarding agent (eg. NXLog, Universal Forwarder, Sentinel Agent)

7.2.9 The Supplier will only leverage the In-Scope Managed Technologies to assist with investigations.

7.2.10 All documentation provided by the Supplier will follow the Supplier template

7.2.11 Any travel expenses will be approved in advance by the Customer and Cyderes shall be reimbursed for such expenses.

7.2.12 The Customer will be responsible for ensuring connectivity between source devices and the SIEM infrastructure

7.2.13 The Supplier will not be required to engage with Customer change management for telemetry or detection engineering

7.2.14 The Supplier will not be required to undergo any formal client training requirements where resources used are part of the leveraged service.

7.2.15 The Supplier will have a single point of escalation for all security Alerts to be sent to. This may be an individual, mailbox, portal or client ticketing solution.

7.2.16 Supplier reserves the right to replace any third-party technologies required to perform the services.

7.2.17 If applicable, product and licensing costs not included in the fees table will be invoiced separately.

7.2.18 For Custom Detection requests, the Supplier may amend the request to ensure Alerts are of high value and create an acceptable Alert volume, and reserve the right to not send custom Alerts to the SOC should the Alert fidelity be deemed low

7.2.19 Supplier makes no warranty that the service will detect every vulnerability, IOC (Indicator of Compromise), IOA (Indicator of Attack), EOI (Event of Interest), External Threat or Internal Threat to the Customer's network, or that the results generated by the services, will be error-free, accurate, or complete.

7.2.20 Supplier cannot perfectly anticipate emerging threats and have detection rules in place covering every scenario.

7.2.21 Supplier shall not be responsible for any changes to the prioritization model by Customer.

7.2.22 In consultation with Customer, Supplier will advise on the number and location of collectors and will help determine if they need to be deployed in the cloud or on-prem. Customer is responsible for deploying the collectors and Supplier will provide oversight.

~~7.2.21~~7.2.23 Customer can request the creation of additional rules via a ticket or request through their CSM.

8. Customer Obligations

8.1 The Customer must identify the Customer Lead prior to the SOW Effective Date.

8.2 The Customer will confirm any access for the Supplier resources be provisioned and confirmed in advance of the Supplier Onboarding team being mobilized.

8.3 The Customer will provide timely access to people (resources from design, implementation, support, and maintenance organizations), information, servers, workstations, and facilities required for Supplier to perform any onsite or off-site activities outlined in this SOW.

8.4 The Customer will provide the Supplier with the requisite administrative or read-only access (as defined by the Supplier) to In-Scope Managed Technologies to provide the Services

8.5 The Customer must have the requisite technology subscriptions to enable the forwarding of data

8.6 The Customer is expected to Deliver any required support such as infrastructure change, agent deployment, device procurement in a timely manner (assumed to be 5 business days).

8.7 The Customer will be required for agent deployment through approved means should agents be agreed to be used.

8.8 The Customer will complete all templates provided by Supplier.

8.9 The Customer must comply with the defined processes.

8.10 The Customer is responsible for the applicable physical environment for the In-Scope Managed Technologies:

- the storage per the manufacturer's specifications;
- the physical condition of the In-Scope Managed Technologies;
- the infrastructure required for the function of the In-Scope Managed Technologies.

8.11 The Customer is responsible for applicable log collection infrastructure and ensuring all applicable Security Events are sent to the Supplier SOC through the SIEM (as defined below) for processing. Supplier will only have visibility into Security Events that are received by the Supplier SOC. Supplier provides additional enrichment related to the security Event using our analytics platform and feeds the Alerts to our SOC.

8.12 The Customer agrees not to tamper with, alter or otherwise rearrange the Services nor shall it permit or assist others to abuse or fraudulently use the Services including, but not limited to, using the Services (i) in any manner which interferes unreasonably with the Services or access thereto by other persons; or (ii) for any purpose or in any manner directly or indirectly in violation of applicable laws or in violation of any third-party rights.

8.13 The Customer shall solely be responsible for use of the Services by any of its employees, officers, directors, agents as well as its end users and agrees to take all necessary measures to ensure that such persons use the Services in accordance with the terms and conditions of this SOW and the MSA.

8.14 The Customer shall be solely responsible for obtaining necessary licenses and/or authorizations for all software and equipment which are not managed or supported by Supplier. Supplier shall not be responsible if any equipment, hardware, or software not managed or supported by Supplier, becomes obsolete, requires modification or attention, or otherwise affects performance of same.

8.15 The Customer shall not, for any purpose, resell or remarket all or any portion of the Services provided under this SOW.

8.16 The Customer shall not engage any Supplier personnel to work on out-of-scope items unless a CO is executed by both parties.

8.17 Failure to perform any Customer Obligations may result in delays and additional costs.

9. Out-of-Scope

Any services not detailed within this SOW are considered out-of-scope including, but not limited to:

9.1 Incident Response beyond containment of Endpoints through In-Scope Managed Technologies

9.2 Device logging remediation (Supplier is not responsible for remediating any issues with the source device)

9.3 Management of the Operating System (OS) of the forwarding infrastructure

9.4 Certificate management or monitoring

9.5 Forwarder management (deployment or management of Endpoint forwarders)

9.6 Raising or configuring network changes to allow data sources to reach Supplier

9.7 Use of Customer technology other than the In Scope Technologies or those which have been integrated with Cyderes SOAR for security investigations

9.8 Any access to or management of Customer technology not explicitly listed in the In-Scope Managed Technologies section of this SOW

9.9 Two-way Ticketing system integration.

[SOW Acceptance page to follow]

Statement of Work

28957 – DeKalb County School District- Managed Services

10.SOW Acceptance

By signing below, each party represents that they understand and agree to the terms of this SOW and are authorized to execute this SOW.

DeKalb County School District	**Cyderes Group LLC**
I have the authority to bind the company:	I have the authority to bind the company:
_____	_____
Signature	Signature
_____	_____
Name Printed	Name Printed
_____	_____
Title Printed	Title Printed
_____	_____
Date Signed	Date Signed

Statement of Work

28957 – DeKalb County School District- Managed Services

Appendix A: Definitions

Except as otherwise indicated, capitalized terms in this SOW have the same meaning as in the Agreement. The following additional definitions and acronyms may apply to this SOW:

Agreement	Master Services Agreement
Alert	A Notification based on analysis of log data or leveraging a broader detection suite that indicates potential attack activity has been detected or directed at an organization's information systems.
Asset	A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.
Build Book	Architectural document detailing the system architecture
Completion Certificate	Document which evidences the effective completion of the Onboarding deliverables
Detection Content	A single correlation search deployed in the Managed Technologies or piece of data added to the intelligence platform
Endpoint	An endpoint is anything an agent can be installed on
Events	An observable occurrence in an information system or network.
Excusable Event	Service Level failures attributable to: (A) the acts or omissions of Customer or its other suppliers acting on behalf of Customer (excluding Supplier and any Supplier subcontractors); (B) a force majeure event, (C) a service outage pre-approved by Customer, or (D) any other event outside of the reasonable control of Supplier or any Supplier subcontractors, provided that in each instance such event (X) did not result from the negligence, fault, or intentional wrongdoing of Supplier; and (Y) could not have been prevented by reasonable foresight or precautions, including through proper execution of Supplier's business continuity or disaster recovery plans or through the use of reasonable workaround plans.
E2E	End to end
Incident	An Alert may become an Incident once investigation has been completed and a determination has been made that there is a high likelihood of malicious activity in the Customer environment. An incident may be able to be resolved by Supplier if relevant delegated authority to implement containment has been given.
Lighthouse	Microsoft 365 Lighthouse is an admin portal that helps Managed Service Providers (MSPs) secure and manage devices, data, and users
Log Source	Any data source within the Customer environment that produces security-event based logs. Log Sources In-scope must log to the Supplier Data Pipeline either via the Supplier Forwarder or a hosted integration.
MSA	Master Service Agreement

Notification	The identification and classification of a notable threat event. It is measured by the time it takes from when a system event is received to when Supplier notifies the Customer through mutually agreed upon communication methods.
Onboarding	The initial phase of the engagement where the Service is made production ready
Operate Phase	The ongoing Manage Service period
OVA	Open Virtualization Format
Playbook	Automated set of processes built in the supplier SOAR solution in response to a Rule triggered via an Incident.
Resolve	The completion of pre-approved manual processes followed by the Customer and/or the Supplier in response to a specific Incident. It is measured from the time an Alert is received to the time pre-approved activities are deemed complete.
Response	An escalation provided to the customer based upon response procedures following initial investigation triage, analysis, and documented recommendations. It is measured from the time an Alert is received to the time the escalation is sent to customer
Rule / SIEM Rule	Signature-based or Correlation.
Runbook	Companion Document for a managed technology, detailing process workflows for any in-scope task.
Services	The In-Scope Managed Services
SIEM	Security Information and event management technology
SOAR	Security orchestration, automation, and response technology
SOW	This Statement of Work
Technologies	The In-Scope Managed Technologies
Telemetry	Valuable Data
Tuning	Process where the functions of a SIEM Rule and/or the priority of the Incident is adjusted.
Users	Users are defined as the total amount of user sensors (laptops, servers, mobile devices) that generate a digital exhaust that is consumed by in scope technologies in place at the company.
Workflow Solution	Any workflow system hosted by the Supplier, which is used to work Events and track tasks

Statement of Work

28957 – DeKalb County School District- Managed Services

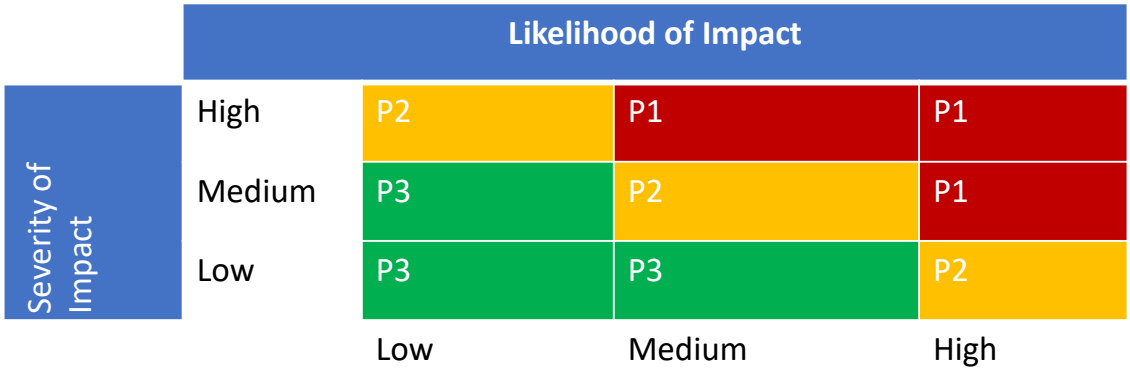
Appendix B: Service Level Objective

Supplier Services include the following Service Level Objectives ("SLO"). All times are measured from the successful receipt of the Event log by the Supplier Cyber Defense Platform.

Service Level	Description	Time
1 – Notification	Notification is the identification and classification of an Event. This is measured from when Supplier receives the Event to when Supplier notifies the Customer through mutually agreed upon communication methods.	**Priority 1**: Up to 30 minutes
		Priority 2: Up to 45 minutes
		Priority 3: Up to 60 minutes
2 – Response	Response is the escalation provided by Supplier to the Customer after the initial investigation triage and analysis of an Event. This is measured from the time an Event is received by Supplier to the time the Alert is resolved as a false positive/ acceptable activity, escalation is sent to Customer or take pre-approved containment actions in accordance with pre-approved Playbooks.	**Priority 1**: Up to 2 hours
		Priority 2: Up to 8 hours
		Priority 3: Up to 24 hours

Priority Level Descriptions

The below image indicates the Supplier approach to categorizing Alerts within the Supplier workflow solution. During Onboarding, and within the Operate phase of service, the Supplier will assess both the severity of impact and likelihood of impact to make an informed decision on the most appropriate Priority rating for the Rule base. The Supplier reserves the right to amend Priorities based upon our adaptable and dynamic priority framework.



SLO Measuring & Reporting

Measuring & Reporting

- SLO's will be measured monthly by Supplier to ensure compliance.
- SLOs will be enforced starting ninety (90) days after the SOW Effective Date, known herein as the SLO Grace Period. Net new Use Cases added during Security Services are subject to an individual reduced SLO Grace Period of two (2) weeks. SLOs may be voided if dependencies and input from Customer is not received in a reasonable and timely manner. Such dependencies and input required may include but are not limited to the Standard Operating Procedures, Asset Classification, Asset Owners.

- SLOs will be enforced starting after the SLO Grace Period. For the avoidance of doubt, SLO's will be tracked during the SLO Grace Period, in addition to the balance of the Term, and used during the SLO Grace Period for informational and tracking purposes.
- Any changes to the shared documentation made by the Customer during the Term require notification to Supplier upon implementation via email to the appropriate Supplier resource. If notification is not received, any SLOs are suspended until such time that Customer sends proper notification of the change.

Service Level Compliance

The following is without prejudice to other rights and remedies:

- Supplier will determine if the missed Service Level is the result of an Excusable Event (the definition of an Excusable Event can be found in Appendix A) and provide the findings to Customer. Customer will not unreasonably withhold or delay its agreement with Supplier's assertion that the missed Service Level resulted from an Excusable Event.
- If Customer and Supplier agree that the missed Service Level resulted from an Excusable Event, Customer may request a Service Improvement Plan to be initiated.
    - If Customer and Supplier do not agree that the missed Service Level resulted from an Excusable Event, both parties will engage in the Escalation Process found in Appendix F.
- Compliance will be calculated and applied as follows:

Category	Compliance
Notification	Compliance to this Service Level means attaining a monthly compliance rate as follows: Priority 1 – 97% Priority 2 – 95% Priority 3 – 90%
Response	Compliance to this Service Level means attaining a monthly compliance rate as follows: Priority 1 – 95% Priority 2 – 90%

Service Improvement

- A SIP will detail the reasonable steps to be taken by Supplier to prevent the missed SLO from reoccurring and will include an estimated number of service days to complete the SIP implementation. If a SIP has been created for either an excusable or non-excusable event, Supplier shall:
    - Provide updates on the status of the SIP implementation at the then agreed upon cadence.
    - Schedule a SIP Close-Out meeting with Customer to confirm the SIP may be completed.

Exclusions

The following items are excluded from the SLO:

- Outages caused by an act or omission of Customer, its agents, or representatives

- Events triggered by an Alert that requires Tuning (or approval for Tuning) by the Customer where the requirement for Tuning was previously requested by Supplier.
- Any request Supplier and Customer agree are non-standard upon validating request
- Any request submitted by someone other than Customer's designated point of contact(s)
- Delays in implementing mitigations caused by an act or omission of Customer, its agents, or representatives, including but not limited to Customer change control processes.

Appendix C: Pricing Terms

a. Payment Terms are Net 30. An additional 1.5% per month late fee charge will apply.

b. All invoices shall be paid within ninety (90) days of invoice including late fee adjustments. To the extent that any amounts are not paid when due, Supplier, upon prior written notice, may suspend the performance of any Services to Customer, without liability, until such payments have been made.

c. Annual Fees are subject to a Cost-of-Living Increase upon renewal.

d. Billing Contact:

Contact Name:
Billing Address:
Phone Number:
Email:

e. All and any taxes are extra. All fees are in USD.

f. All billable travel expenses will be at cost only, subject to Customer approval.

g. Should the scope of the service or costs to procure licenses for the In-Scope Managed Technologies increase or decrease, then, for any Renewal Term, Supplier reserves the right to amend the Fees by providing Customer prior written notice of the Fee change before the end of the Initial Term or applicable Renewal Term. For clarity, both parties will discuss in good faith prior to any changes.

h. The number of Active Users shall be calculated quarterly on the first day of the current quarter.

   a. The Active User count is assumed to be at 15,000 Users. The definition of Users is specified in Appendix A.

   b. Should Customer's Maximum Active Users exceed the current license, then, the corresponding additional service overage charge (User package) will be applied for the current quarter and immediately invoiced for the remainder of the current year. Once applied, additional service overage charges are applicable for the remainder of the Term.

Packages	User Counts	Overage Charges
Current	Up to 15,000 Users	No Additional Charges
Additional Active Users	1,000 Users	Additional $45,000.00 per year

Appendix D: Log Source Tiers for Onboarding

Supplier's intention is to onboard up to 8 Tier-1 data sources for initial Onboarding. Completion of Onboarding Services is not tied to the Onboarding of all the below Log Sources, as some will not be applicable. The Customer is not obligated to complete this in advance of signature; however, this will expedite the Onboarding capability.

For security relevance, not all logs are created equal. Some products provide more value for detecting hostile activity and align better with our rules and the services we provide. Like clients, the kind of telemetry needing support are broken into three categories (tiers) of which Tier 1 & Tier 2 are provided below:

- **TIER I - Mission Critical Primary Security Log Sources**: These are Log Sources that generate "first order" and "high fidelity signal" cybersecurity Alerts from EVERY customer environment.
- **TIER II - Secondary Security Log Sources**: These are Log Sources that generate "lower fidelity signal" cybersecurity Alerts or provide raw logs for our own custom detections

Controls	Named Technology & Version	Cyderes reference	Onboarding Deliverable?
Tier I (Critical Controls)			
Endpoint (EDR or Legacy AV)			Yes/No
Authentication/ Single Sign On/ Privileged Account Monitoring			
Secure Email Gateway (SEG)			
CSPM (Threat Only, No Vulnerability or DevOps Alerts)			
Proxy			
Tier II (Important Controls)			
Firewalls			
Web Application Firewall			
IDS/IPS			
VPN			
Network Access Control			
Operating System & Security Logs- Windows			
Operating System & Security Logs – Linux			
Operating System & Security Logs - Mac			
Security/Audit Logs from SaaS applications			
Encryption / HSMs			
Data Loss Prevention (DLP)			
Customer DNS Domain Names (monitoring typo-squatting)			

Appendix E: Urgent Major Incident Response Services

Customer can request Urgent Incident Response Services via this SOW. This is not an included Service. A new SOW will be drafted and signed by both parties with costs applied.

a. Customer has an Urgent Incident Response Rate of $450.00 per hour.
b. Urgent Incident Response Services can be authorized to start work via email or voice call. A separate SOW will be drafted in tandem with the services being delivered.
c. Urgent Incident Response Services require a minimum project of twenty-four (24) hours per engagement when team resources are deployed. Initial calls do not activate this minimum. In the interest of immediate response services, Customer consents to an initial invoice for $10,800.00 for work requested.
d. Initial advice and scoping will follow as soon as possible from the initial request. Subject to travel restrictions, on-site response may be available. On-site service, if available, requires minimum of eight (8) hours multiplied against the Urgent Incident Response Rate per day including travel times. Supplier may apply GSA mileage. Supplier may apply per diem rates and usages within the United States in place of actuals expenses.
e. Following a triage period, typically two (2) to three (3) working days but conditions encountered may prolong the triage period, an initial estimate will be provided to Customer in the form of a SOW draw down. The initial estimate is offered in good faith but may be altered due to changes in scope. Potential scope changes include additional systems, additional requests in support of Customer, or Customer counsel requests.
f. Customer may direct Supplier to stop work at any time during the provision of Urgent Incident Response Services. Upon receiving such a request, Supplier may require additional hours to end processes and dispose of data but shall not exceed sixteen (16) additional Hours. Customer acknowledges that Supplier may require additional Hours to complete a report. Supplier cannot commit to provide interim written reports at the time of the stop work notification without a full Quality Assurance process.

Appendix F: Processes

Change Management Process.

The Supplier will perform Moves/Adds/Changes as requested by the Customer as a CIR (Customer Initiated Request):

a. Unless specifically state otherwise, Supplier limits the number of total CIR's to three (3) per month with exceptions to emergency requests (do not count toward limits).
b. CIR's must be made through Supplier Customer Portal and must be scheduled for requests estimated to be complete with three (3) hours of work effort.
c. CIR's will only be actioned during Customer regular business hours and will follow the defined Change Process unless mutually agreed upon by Customer and Supplier during off-hours.
d. Requests are subject to rejection by the Supplier after review if deemed unrelated to the Services or based on recommendation by the Supplier, rejection shall not be unreasonably withheld.
e. Supplier will develop a Change Management Process based on Customer's internal process.
f. CIR's cannot be bundled and cannot be carried over to the following month if unused.
g. A list of requests has been provided below:

- Add, Modify, Disable, Delete User/User Role
- Disable/Delete Log Source
- Update/Modify existing configuration.
- Configure back-up of on-premises SIEM
- Rotate admin credentials

Problem Management.

a. Customer will direct any complaints to the general service via communication to the Customer Success Team (via ticket or email). If not resolved at the Customer Success level, the escalation moves to the Director level. If still dissatisfied with the resolution, Customer can contact VP level leadership.
b. Formal complaints can be logged with the Supplier corporate body at any time. Contact channels will be provided and shared in the shared Knowledge Database.
c. Customer Success will draft a "Get to Green" roadmap for any complaint leading to Customer dissatisfaction with the overall Services. A Get to Green roadmap will be attached to a ticket and/or reviewed in a customer operational meeting following standard milestone tracking. Green status (resolution and closure) requires completion of agreed to roadmap deliverables.

SOW Change Order Process:

a. This service has defined deliverables detailed in this Statement of Work. If a change outside this Statement of Work affects the performance, functionality, cost, delivery date, or other technical parameter of a deliverable, or if Customer delays the service schedule for any reason or is unable to fulfill its responsibilities defined in this Statement of Work, and if such a change results in increased cost to Supplier, then a change order will be submitted and processed using a CO. Customer will not initiate or engage the Supplier consultant to work on out-of-scope items without prior approval of a CO.
b. Either Supplier or Customer may initiate a change to the service. The cost, scope, and any schedule impact of the change will be analyzed and documented. The change impact will then be processed for Customer authorization or closure.

c. If Supplier and Customer are unable to agree on the terms of the change order, then the service scope and activities will remain as defined in this document.

Document Review Process:

a. When Supplier provides documentation as part of the service, each document deliverable will initially be developed in draft form. When the draft document is complete, the Supplier will submit the initial release document to Customer assigned owners for review and comment.
b. Customer owner will be responsible for distributing copies of the initial release document for internal review. The Customer reviewer is responsible for consolidating all Customer comments and for providing a clearly marked version of the draft document to the Supplier.
c. Customer owner will have ten (10) business days to review and return the consolidated comments to the Supplier, unless otherwise agreed to by the parties. If a response is not received within ten (10) business days from the Customer owner, documents will be deemed approved and completed. Supplier will review and evaluate Customer comments and schedule resource to respond to them.

Offboarding Procedures:

If Customer decides not to renew or cancels but would like to migrate (duplicate) all the use cases for a new provider or for them to take in house the following steps would occur:

a. Removal of any Supplier proprietary applications.
b. Supplier will not remove the Use Case configured Alerts.
c. Support to migrate existing Use Cases to a new SIEM or Service Provider can be delivered at an additional cost.
d. Supplier will provide Customer with a backup of Customer data (in an agreed format) and once received, Supplier will securely delete Customer data from Supplier systems as per Supplier's SOC II audit and data retention requirements.

Appendix G: Terms and Conditions

Confidentiality.

a. Each party (the "Receiving Party") acknowledges that, by virtue of and in the course of performing its obligations under this SOW or Purchase Order, the other party (the "Disclosing Party") may provide the Receiving Party with, or the Receiving Party may otherwise access or become aware of proprietary or Confidential Information relating to the Disclosing Party or its affiliates, suppliers, and clients (including the identity of such clients). During the term of the SOW and at any time after the expiration or termination of the SOW, the Receiving Party will keep in strict confidence all Confidential Information of the Disclosing Party. "Confidential Information" means information, materials or data obtained, accessed, disclosed, used, or acquired in connection with the SOW that is non-public. The Confidential Information will be used for no purpose other than for the Receiving Party to exercise its rights and fulfil its obligations under the SOW.

b. Section (a) shall not restrict the Receiving Party from disclosing Confidential Information of the Disclosing Party (1) if disclosed to its affiliates, lawyers, accountants, auditors, managers, representatives, contractors, employees and consultants who have a need to know the Confidential Information in furtherance of the purpose set forth in the Agreement (collectively, the "Representatives"), provided that, prior to the Receiving Party disclosing Confidential Information to its Representatives (i) such Representatives are informed by the Receiving Party of the confidential nature of the Confidential Information and the obligations in this SOW, and (ii) such Representatives are subject to written confidentiality obligations similar to the confidentiality obligations set out in this SOW, and in all instances each party will be responsible for its Representatives' compliance with the foregoing, or (2) to the extent required by applicable law, court order or a requirement of an applicable regulatory or administrative authority upon prior written notice to the other party (to the extent practicable and permitted by law).

c. Confidential Information excludes information which: (a) is rightfully in the Receiving Party's possession without breach of this section; (b) is or becomes generally available to the public other than as a result of a violation of this section; (c) is lawfully received by the Receiving Party from a third-party that the Receiving Party knows is not prohibited or limited from disclosing such information; or (d) is independently developed by the Receiving Party or its Representatives without any use of or reference to the Confidential Information.

Disclaimers. Limitation of Liability.

a. CUSTOMER ACKNOWLEDGES THAT SUPPLIER MAKES NO REPRESENTATIONS, WARRANTIES OR CONDITIONS OF ANY NATURE, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, RESPECTING THIRD-PARTY PRODUCTS AND THE SERVICES AND DELIVERABLES PROVIDED BY SUPPLIER, INCLUDING BUT NOT LIMITED TO NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR FROM A COURSE OF DEALING OR USAGE OF TRADE. CUSTOMER ACKNOWLEDGES THAT SUPPLIER IS NOT THE MANUFACTURER OR ORIGINAL PROVIDER OF THE THIRD-PARTY PRODUCTS AND DID NOT SELECT THE THIRD-PARTY PRODUCTS AND THAT CUSTOMER HAS MADE THE SELECTION OF SUCH THIRD-PARTY PRODUCTS BASED UPON ITS OWN JUDGMENT AND SUPPLIER EXPRESSLY DISCLAIMS ANY CUSTOMER AND ITS AFFILIATES RELIANCE ON STATEMENTS MADE BY SUPPLIER OR ITS AGENTS.

b. To the extent applicable, Supplier shall assign to Customer any manufacturers' warranties for the third-party products sold hereunder.

c. In no event shall either party's aggregate liability in connection with a Purchase Order or SOW exceed the amounts actually paid by Customer to Supplier in aggregate over the immediately preceding twelve (12) month period preceding the first incident out of which the liability arose. Notwithstanding the foregoing, in no event will Supplier's liability in connection with the third-party products exceed the limitation of liability offered by any supplier of such third-party products, which limitations of liability pass through to Customer pursuant to the terms

of any such third-party supplier contractual documentation or equivalent instrument.

d. THE LIABILITY OF EITHER PARTY FOR ANY BREACH OF THE SOW OR PURCHASE ORDER OR OTHERWISE FROM ANY ACTS OR OMISSIONS OF ITS RESPECTIVE PERSONNEL WILL IN ALL CIRCUMSTANCES BE LIMITED TO DIRECT DAMAGES AND IN NO EVENT WILL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER, WHATSOEVER, FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR PUNITIVE DAMAGES OF ANY KIND ARISING OUT OF THE MSA, A STATEMENT OF WORK OR A PURCHASE ORDER, OR FOR LOST PROFITS OR FOR THE COST OF PROCUREMENT OR SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR OTHERWISE EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Indemnification.

a. Supplier shall indemnify Customer and its affiliates and its and their officers, directors, employees, agents and representatives and save them fully harmless against and will reimburse them for any third-party loss, cost, liability, claim, interest, fine, penalty, assessment, damages or expenses arising from, in connection with or related in any manner whatsoever to any claim that the Services, including deliverables (but excluding third-party products), infringe any intellectual property right in Canada, the United States or the United Kingdom, or misappropriates a trade secret and shall pay all damages awarded or agreed to under a settlement made by Supplier and/or by a court of final appeal attributable to such claim, provided Supplier (i) receives prompt notice of such claim provided that failure or delay or alleged delay in providing such prompt notice shall not adversely affect Customer's right to indemnification hereunder, unless and then only to the extent that such failure or delay or alleged delay has resulted in actual prejudice to Supplier, including, without limitation, by the expiration of a statute of limitations, (ii) has sole control over the defense and/or settlement of such claim (with Customer retaining the right to participate in such claim (but not control) with its own counsel, at its own expense), and (iii) receives all reasonable cooperation and assistance from Customer with regard to such claim.

b. Customer shall indemnify Supplier and its affiliates and its and their officers, directors, employees, agents, and representatives and save them fully harmless against and will reimburse them for any third-party loss, cost, liability, claim, interest, fine, penalty, assessment, damages, or expenses arising from, in connection with or related in any manner whatsoever to any Customer act, error or omission.

Non-Solicitation

a. Neither party will, without the express consent of the other party in each instance, during the term of the Agreement and for a period of twelve (12) months thereafter, directly, or indirectly solicit, employ, offer to employ, or offer to engage as a consultant, any employee or independent consultant of the other party with whom such party had contact pursuant to the Agreement. The foregoing prohibition will not apply to prevent either party from soliciting any such employees of the other party in any of the following situations: (a) through advertisements or general solicitations not specifically targeted at such employees; (b) if the employee was terminated by the other party or resigned from his or her position on his or her own initiative and without the hiring party's affirmative act to induce or contact the employee; or (c) where the employee contacts the hiring party on his or her own initiative and without the hiring party's affirmative act to induce or contact the employee.