TOOELE COUNTY CORPORATON
CONTRACT # 20-10-12

SECUVANT
Cyber Security | Risk Management

Tooele County | COA-RL20200916-1B

CHANGE ORDER: ADDENDUM TO EXISTING SERVICES

This change order ("Addendum"), with an effective date of October 1, 2020 ("Addendum Date"), modifies the original Managed Security Services Agreement "Proposal ID MDR-GJ20180420-1B" with an Effective Date of May 1, 2018, (the "Agreement"), made by and between Secuvant LLC, ("Secuvant") whose address is 9067 S 1300 W #305, West Jordan, Utah 84088 and Tooele County ("Client"), whose address is 47 South Main Street, RM # 125, Tooele, UT 84074; herein referred to as the ("Original Agreement").

WHEREAS, Secuvant and Client (collectively referred to herein as the "Parties") wish to modify the service item(s) of the Original Agreement as set forth herein.

NOW THEREFORE, the undersigned Parties do hereby agree to modify the Original Agreement as per the Line Item Summary, Exhibit A, and Exhibit B included herein. Furthermore, the Original Agreement shall be modified to change the meaning of "Client" to Tooele County per the Acceptance Section of said Agreement. No other terms or conditions of the Original Agreement shall be negated or changed as a result of this Addendum; notwithstanding the foregoing, in the event of any inconsistency or conflict between the Original Agreement and this Addendum, the provisions of this Addendum shall govern and control.

Line Item Summary	Quarterly Fee
Original Agreement Fee:	$22,280
Change to Services ("Services"): Per Exhibit A; highlights include increasing Agent quantities from 50 to 87 and Updating SLA's	$2,586
New Rate ("Rate"):	$24,866
One-Time Onboarding Fee (if applicable): Not Applicable	$0
Modified Term ("Term"): Addendum shall co-term to existing contract term date	Co-Term

SERVICE START AND FEES: Changes to the Services, Rate, and Term shall take effect upon the Addendum Date of this Agreement. The adjusted Rate for Services shall be invoiced immediately upon acceptance and shall be due upon the Addendum Date.

ACCEPTANCE: In witness whereof, the Parties hereto have caused this Addendum to be executed by their duly authorized representatives as of the Addendum Date, wherein this change order, with its accompanying exhibits, shall become a legally binding agreement, being incorporated into the Original Agreement upon the execution of both Parties:

Secuvant	Client
Signature:	Signature:
Name:	Name: Tom Tripp
Title:	Title: Tooele County Commission Chair
Date:	Date: 19 Oct 2020

EXHIBIT A: SECUVANT SERVICE SUMMARY

MANAGED DETECTION AND RESPONSE	OPTION A
Service Level Agreements	
SOC Event Monitoring | Threat Hunting | Critical Event Response	24/7/365
Tier 4 Escalated Incident Response & Forensics	30 Min
Network Data Retention	30 Day
Log Retention	400 Day
Managed SIEM	
Collection Points	1
Tier 1 Agents - Workstation | Switch | Router	-
Tier 2 Agents - Server | Syslog	87
HoneyNet Deception - 25 Servers	-
Managed Network Threat Monitoring	
Network Threat Sensor Locations	4
Full PCAP Add-on - Optimized Bandwidth (Mb/s)	3
Managed Vulnerability Scanning	
Internal Scans - Unique Scans	1
Internal Scans - Active IPs	666
Scan Cadence	Quarterly
External Scans - Active IPs	7
Scan Cadence	Quarterly
PCI Scans - Active IPs	-
Scan Cadence	-
Managed EDR	
Endpoint Agents	-
MANAGED RISK SERVICES	
Risk Program Management	
Risk Program Manager	✓
vCISO Hours - Monthly	8
Roll Over Hours	90 Days
Risk Program Acceleration	
Security Gap & Risk Assessment	-
Cyber Risk Executive | Board Workshop	-
Strategic Security Road Map Creation and Execution	-
Risk Program Validation	
PenTest Engagement Type	-
PenTest Duration - Weeks	-
PenTest Cadence	-
Security Awareness Training	
Total Users	-
Managed	-
SERVICE FEES	
Managed Detection & Response - Monthly Fee	$16,247
Managed Risk - Monthly Fee	$8,618
Combined Services - Monthly Fee	**$24,866**
One-time Implementation Fee	$0
Agreement Term	Co-termed to Existing

EXHIBIT B: SERVICE LEVEL AGREEMENT

Introduction

This Service Level Agreement ("SLA") document defines the service levels associated with the Agreement and are subject to the Agreement's Terms and Conditions as previously set forth. These SLA's, including supplemental processes and definitions, make up the framework and structure of this Managed Security engagement between Client and Secuvant.

Initiating a Service Ticket

Secuvant has three (3) methods for initiating a ticket for an actionable security event (an "Event"):

- METHOD 1 - Secuvant creates a ticket manually or auto-creates tickets via its monitoring tools
- METHOD 2 - Client sends an email to support@secuvant.com
- METHOD 3 - Client calls (855) 732-8826, Option 1 to be connected to Secuvant Analysts

Service Level Agreements

Secuvant manages Service Levels for (i) Monitoring & Alerting and (ii) Event Response Time:

- Monitoring & Alerting SLA: Secuvant provides threat hunting, monitoring and alerting 24/7. Alerts are prioritized and queued as Events based on the following severity levels: CRITICAL, HIGH-PRIORITY, MEDIUM-PRIORITY, and LOW-PRIORITY. Secuvant's subsequent response to an Event is governed by the severity of the Event Response Time SLA.
- Event Response Time SLA: CRITICAL support tickets are co-managed with the Client 24/7; all other severity levels are co-managed Monday-Friday, 6am-6pm MT, excluding holidays. Severity level definitions and Response Time SLA's are summarized below:
    - SEV-1: CRITICAL – Defined as a vulnerability, or viable incoming threat to exploit that vulnerability which, if exploited would allow malicious native-code to execute, potentially without a user being aware; or a validated monitoring event occurs that is deemed by Secuvant to be an eminent threat to Confidentiality, Integrity or Availability of the Client's Systems or Network. For an Event classified as CRITICAL, a ticket will be created immediately upon verification via one of the methods listed above, with a response from an Analyst taking place within 1 Hour of Secuvant receiving the alert. Client should act upon alerts with urgency and communicate with Secuvant immediately.
    - SEV-2: HIGH PRIORITY – Defined as a vulnerability, or an incoming threat which, if exploited could compromise data security, potentially allowing access to confidential data or system

compromise as assessed by Secuvant Analysts. For an Event classified as HIGH PRIORITY, a ticket will be created immediately upon verification via one of the methods listed above, with a response from an Analyst taking place within 4 hours of Secuvant receiving the alert. Client should act upon alerts with one business day and communicate to Secuvant at its earliest opportunity.

- SEV-3: MEDIUM PRIORITY – Defined as a vulnerability or potential threat, that is limited to a significant degree by factors such as default configuration, auditing, system configuration, architectural integrity, or is difficult to exploit. For an Event classified as MEDIUM PRIORITY, a ticket will be created immediately upon verification via one of the methods listed above, with a response from an Analyst taking place within 24 hours of Secuvant receiving the alert. Client should act upon alerts within 3 business days and communicate to Secuvant as appropriate.
- SEV-4: LOW PRIORITY – Defined as informational by design, with little to no impact on an organization's systems. Business relevant information from Secuvant is communicated through this severity level. For an Event classified as LOW PRIORITY, a ticket will be created immediately via one of the methods listed above, potentially without some details required in other Severity Levels. For the Client, there is no expectation of a response to Secuvant for a Low Priority ticket.

Holidays Observed

Holiday	Date
New Year's Day	January 1st
Memorial Day	Last Monday in May
Independence Day	July 4th
Labor Day	1st Monday in September
Thanksgiving Day	4th Thursday in November
Christmas Day	December 25th

Risk Management Hours - Monthly

The Agreement includes a fixed number of hours at a Base Rate of $200 per hour. Hours are tracked in 15 minute increments and accrue as a multiple of the Base Rate per the Consultant Role and Work Type. Hours not used during a given month carry-over for a period of **90 days** and are then retired; hours used beyond the allotted contract amount are billed monthly in arrears.

Consultant Role

Consultant Role	Base Rate Multiple
Consultant	0.75
Senior Consultant (Base Rate)	1.00
Managing Consultant	1.25
Principal Consultant	1.50

Work Type

Name	Description	Rate
Business Hours	Time accrued during business hours – 6am–6pm MT	Base Rate Multiple
After Hours	Time accrued after hours – 6pm–6am MT	Base Rate Multiple + 25%
Holiday Hours	Time accrued during Observed Holidays	Base Rate Multiple + 50%

Incident Response and Forensics Engagement

Secuvant has partnered with best-in-class Incident Response organizations ("IR Partner") that specialize in breach response support, forensics analysis, ransomware negotiation, restoration, and dark web research. In the event a Secuvant MDR investigation reaches escalated status, Secuvant will engage its IR Partner at no additional charge to Client to assist with breach analysis, scope, and triage. Should Incident Response and Forensic services be required by Client, Secuvant will initiate direct engagement between Client, Client's External Counsel, and the IR Partner. Secuvant proceeds to support IR Partner in performing the following breach response services (as required):

- **Ransomware, Decryption and Decryption Validation** - Provide support for ransomware negotiation, bitcoin payment and decryption software validation support

- **Incident Response Support** - Provide support for the overall Investigation effort including recommendations, validation of measures taken, review of architecture and security controls and malware specific mitigation measures.
- **Forensics Analysis Artifacts and Malware** – Perform analysis on available logs looking for malicious behavioral patterns and evidence of exfiltration or access of sensitive data. Additionally, perform forensics analysis on in-scope systems including root cause analysis, malware specifications, and potential compromise or exfiltration of data.
- **Restoration Services** - Provide cyber security team engineers to assist remotely with overall restoration/decryption efforts.
- **Dark Web Search** – Conduct comprehensive retroactive search for Client's data across 1,500+ dark and surface web sources.

Discounted rates for IR Partner services are pre-negotiated with most leading cyber liability insurance carriers. Incident Response fee-based services are governed and controlled by separate Statements of Work, with their accompanying Terms and Conditions, by and between Client and IR Partner.