Managed Detection & Response - Terms and Conditions Schedule

In addition to the Service Agreement between KINETIC BUSINESS and Customer, including any document incorporated by reference therein (collectively the "Agreement"), of which this Schedule is a part, Customer agrees that the following terms and conditions apply to the Managed Detection & Response ("MDR") Service provided to Customer by KINETIC BUSINESS. Unless otherwise defined herein, capitalized terms shall have the same meaning as defined in the Agreement.

1. MDR Service - Definitions. The following definitions apply to the MDR Service features outlined in Section 2(a) below:
   - Firewall – Stateful inspection with support for network address translation and demilitarized zone (DMZ). Firewall policies are defined leveraging port, protocol, and IP address.
   - Virtual Private Network ("VPN") – Site to site VPN Tunnels use Internet protocol security ("IPsec") for VPN connectivity. Standard support for up to one hundred (100) IPsec connections per location firewall instance.
   - Remote Access (Remote Access VPN + Soft Tokens (MFA/2FA)) – End user VPN (IPsec, secure sockets layer ("SSL"), and/or soft tokens) connectivity. Online interface available for Customer to manage end user accounts (i.e. username and password). Integration with Customer-owned and managed Microsoft directory service ("Active Directory") for end user authentication is also supported.
   - Application Control – Identifies common layer 7 web applications for reporting and incorporation in firewall policy for enforcement.
   - Intrusion Prevention System ("IPS") – Focused signature library to protect against network attacks.
   - Web Content Filtering & URL Filtering – Control of web access by end users via predefined and curated site categories and site level support for allow or block list.
   - Threat Monitoring – Monitors security events detected by security information and event management ("SIEM") platform, which collects log data from MDR Firewalls and the pre-qualified customer owned devices ("Customer Device"). The categories of Customer Device that KINETIC BUSINESS supports are Active Directory, Windows Server, and Unix/Linux Server. The default log retention provided as part of the Threat Monitoring is twelve (12) months. Security incidents are stored for the lifetime of a customer.
   - CPE – Customer premises equipment.
   - Gateway Antivirus – Detecting and blocking known viruses in network traffic traversing the MDR Firewall.
   - Incident - Series of events that trigger rules that are based on pre-defined condition or circumstance (e.g., attempted, or actual unauthorized access, use, disclosure, modification, or destruction of the monitored Customers systems or information).
   - SOC – A Security Operations Center is a centralized facility or team responsible for monitoring, detecting, analyzing, and responding to security incidents and mitigating security threats.
   - Device Availability Monitoring – refers to the process of continuously monitoring the availability and uptime of the Firewall CPE
   - Upgrade & Patch Management – refers to the policies that define the procedures for testing, deploying, and verifying patches across you're the Firewall CPE devices
   - Change Management – refers to the processes when applying updates or patches to CPE firewall devices. This includes documenting the changes, notifying relevant stakeholders, and having a rollback plan in case any issues arise during or after the update process.
   - FortiConverter - is a tool provided by the CPE Firewall manufacturer that allows for the conversion of third-party firewall policies and configurations to the firewall platform

2. Description of MDR Service.
   MDR CPE is a premise based MDR Service that leverages a security appliance installed on the Customer's premises. The security appliance is procured, activated, and managed remotely to deliver the MDR Service. HA is available as an option by implementing two (2) security appliances in active/passive configuration.

MDR CPE is available in the following tiers:

Feature	Essentials	Premier
Dedicated Security Operations Center (SOC)	+	+
Firewall Device Availability Monitoring	+	+
Upgrade and Patch Management	+	+
Change Management	+	+
Application Control	+	+
DMZ Network	+	+
Convert Existing FW Configuration	+	+
Active Directory Integration	+	+
Intrusion Detection/Prevention (IDPS)	+	+
SIEM: Threat Monitoring & Log Retention	+	+
Weekly Logs & Reporting		+
Web Content Filtering & URL Filtering		+
Gateway AV		+
Additional Purchase Features		
Remote Access VPN + Soft Tokens (MFA/2FA)	+	+
Site to Site VPN Tunnels	+	+

3. MDR Service Activation. Once MDR Service is ordered, KINETIC BUSINESS will determine the MDR configuration based on a questionnaire form (the "Form") to be completed by the Customer. A KINETIC BUSINESS technical design engineer ("TDE") will complete the configuration form and then a ("SOC") engineer will then configure and activate the MDR Service via a scheduled activation call with the Customer.
4. MDR Service Support. SOC provides 24x7 support to aid Customers in questions regarding the MDR Service, issue resolution, or change requests.
5. MDR Service Availability - MDR CPE's default setup is comprised of a single security appliance installed at the Customer's facility. If the service becomes unavailable due to a device failure, a replacement device will be shipped next business day to Customer's location and installed remotely when received. A HA option is available to prevent downtime due to device failure.
6. Service Level Objectives shall be as set forth in **Exhibit 1**, attached hereto and incorporated herein by reference.

7. Customer's Obligations. Customer agrees to:

- (i) reasonably cooperate with KINETIC BUSINESS and provide the Form and additional information regarding Customer's systems and applications that are connected to MDR to help tuning of monitoring as requested;
- (ii) ensure information for all authorized points of contact remains current;
- (iii) notify KINETIC BUSINESS of any network security architecture changes (e.g. unscheduled back-ups, anticipated increase in legitimate inbound web traffic) that could generate false alerts at least twenty-four (24) hours before such a change; and
- (iv) provide estimated log volume and/or average events per second of Customer Device when Threat Monitoring is required to monitor the Customer Device.

8. MDR Authorized Use. Excessive log volume of Threat Monitoring may have a severe impact on SIEM performance, so the log volume of Threat Monitoring per device should be no more than an average of ten (10) events per second ("Max EPS"). Customer must consult with the SOC before maintaining a log volume over the Max EPS. KINETIC BUSINESS reserves the right to modify, terminate or otherwise amend the MDR Service if the Customer is in breach of this Section 7 and/or if Customer's excessive log volume damages the MDR Service.

9. Exclusions, Limitations and Restrictions

- (a) Any equipment provided by KINETIC BUSINESS as part of the MDR Service remains the property of KINETIC BUSINESS and must be returned to KINETIC BUSINESS upon termination of MDR Service in accordance with the terms and conditions of the Agreement. The security appliance provided by KINETIC BUSINESS will be managed and maintained solely by KINETIC BUSINESS and Customer will not have direct terminal access to the security appliance when KINETIC BUSINESS is responsible for configuration management. Any cold spare equipment obtained through the MDR Service will not receive any firmware or configuration updates. Out-of-territory locations (i.e. geographic locations in which KINETIC BUSINESS does not have a field operations presence) will receive best-effort break/fix and issue resolution support, regardless of purchased MDR Service tier.
- (b) Customers who provide Customer-owned equipment for the MDR Service will not receive support from KINETIC BUSINESS and are responsible for contacting the equipment manufacturer to place a service request when a hardware failure determination is made by KINETIC BUSINESS.
- (c) Antivirus Protection is a discretionary MDR service capability that automatically scans, deletes and removes known computer software virus from network traffic that traverses the firewall with the following exclusions, limitations and restrictions:
    - i MDR Antivirus protection is an optional feature of MDR and requires pre-approval by KINETIC BUSINESS before it's enabled.
    - ii MDR Antivirus protection provides additional layer of protection from Malware (i.e. malicious software) including computer viruses.
    - iii MDR Antivirus protection uses third-party vendor threat information databases for timely updates on the latest malware, virus, and other cyber threat definitions.
    - iv MDR Antivirus protection does not provide protection from zero-day vulnerability where software or hardware vulnerability is known but no patch exists.
    - v MDR Antivirus Protection isn't a substitute for a reliable and up-to-date endpoint* security (i.e. Antivirus) software.
    - vi Antivirus technology is not error free, especially against unknown threats.
    - vii Customer should use endpoint security on all their devices* with Internet connectivity.
    - viii Customer should maintain their endpoint security software with the latest malware, virus and other cyber threat definitions.
    - ix KINETIC BUSINESS does not provide endpoint security software for devices as part of the MDR service *Technology used by organization including but not limited to PCs, Laptops, Tablets, Smartphones and IoT (Internet of Things) devices

10. Authorization to Perform Testing. Customer grants KINETIC BUSINESS the authority to access Customer's networks and computer systems solely for the purpose of providing the Managed CPE Firewall Service ("Firewall"). Customer agrees to notify KINETIC BUSINESS and obtain any third-party service provider's ("Host") consent to provide the Firewall on Host's computer systems, which includes acknowledgement of the risks and acceptance of the conditions set forth herein and to facilitate any necessary communications and exchanges of information

between KINETIC BUSINESS and Host in connection with the Firewall. Customer agrees to indemnify, defend and hold KINETIC BUSINESS and its suppliers harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees that arise out of Customer's failure to comply with this Section and from any and all third-party claims that arise out of the testing and evaluation of the security risks, exposures, and vulnerabilities of the IP Addresses that Customer provides. Customer acknowledges that the Firewall entails certain risks including the following possible negative impacts:

- (i) Excessive log file disk space may be consumed due to the excessive number of log messages generated by the Firewall.
- (ii) Performance and throughput of networks and associated routers and firewalls may be temporarily degraded.
- (iii) Degradation of bandwidth; and customer computer systems may hang or crash resulting in temporary system unavailability and/or loss of data.

11. Customer agrees to the following infringement terms by purchasing the MDR solution:
    - (i) Customer must comply with the Windstream and Windstream partner design.
    - (ii) Customer does not modify the design.
    - (iii) Customer provides prompt notice if aware of a claim of Intellectual Property (IP) Rights infringement claim implicating MDR Service.
12. Intellectual Property Protection:
    - All right, title and interest in and to all copyrights, trademarks, trade secrets, patents, mask works, deliverables, and all other intellectual property embodied in the Products and any documentation produced by us in connection with the Products, including but not limited to written reports, user manuals, training materials and any improvements thereto or goodwill associated therewith ("Deliverables") are retained by us or our licensors. All rights not expressly granted to Customer are reserved and retained by SilverSky and its licensors.
    - Customer will not (and will not allow any third party to):
        - (i) except to the extent applicable law expressly gives you permission to do so, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of any Products (except to the limited extent that applicable law prohibits reverse engineering restrictions);
        - (ii) provide, lease, lend, disclose, use for timesharing or service bureau purposes, or otherwise use or allow others to use for the benefit of any third party, any Products (except as expressly and specifically authorized by us in each instance) or
        - (iii) use the Products, including any documentation provided by us, in connection with the development of products or services that compete with the Products.
    - To the extent Customer provides feedback to Windstream with respect to the Products, Customer grants Windstream and its vendor(s) an unlimited, irrevocable, world-wide, transferable, perpetual, sublicensable, royalty-free license to use such feedback for any purpose, provided use of such feedback does not include Customer's marks.
    - Subject to the terms of this Agreement, Windstream grants Customer the non-exclusive, non-transferable right to access and use the MDR Portal for the limited purpose of facilitating activities under this agreement.

KINETIC BUSINESS is not providing Information Technology ("IT") consulting services and the configuration of Customer's firewall, or any other IT systems, is the sole responsibility of Customer. Prior to the installation or use of the Generic Configuration, Customer should seek the advice and support of its own IT professionals or contractors as needed. KINETIC BUSINESS may offer, upon written request from the Customer and at KINETIC BUSINESS's sole option, a non-specific, pre-configured, generic configuration ("Generic Configuration") to Customer to aid in setting up the Customer's MDR Firewall. Such Generic Configuration is provided "as is" without warranties of any kind and KINETIC BUSINESS expressly disclaims any and all liability arising from Customer's use of a Generic Configuration provided by KINETIC BUSINESS to set up the MDR firewall. Further, Customer agrees to indemnify, defend, and hold KINETIC BUSINESS and its suppliers harmless from and against any and all claims, losses, liabilities, and damages, including reasonable attorney's fees, that may arise out of the testing and evaluation of the security risks, exposures, and vulnerabilities of the generic configuration that KINETIC BUSINESS provides for Customer's use.

Exhibit 1

Service Level Objectives

The Service Levels listed below will apply to the Services as of the first day of the first whole calendar month after the initial installation of the Service deployment.

- Priority Level 1 is defined as a site, platform, or customer-wide, unplanned interruption of a service line for which there is no work around.
    - A call is required to report P1 tickets to Support.
    - A support analyst or engineer will open and work ticket within 5 min
    - Ticket updates every 30 min
- Priority Level 2 is defined as a service or customer-wide, unplanned interruption rendering a service line unavailable, for which there is a work around available.
    - A call is required to report P2 tickets to Support.
    - A support analyst or engineer will open and work ticket within 5 min
    - Ticket updates every hour
- Priority Level 3 is defined as an unplanned interruption rendering services unavailable, for a single user or small percentage of users.
    - Ticket updates every 4 hours
- Priority Level 4 is the default priority that your ticket will be assigned for standard move/add/change requests.
    - A standard ticket is addressed within 4 hours and tickets will be updated as information is available.