Parker Data & Voice, LLC
Technology For Your Business

SERVICE ATTACHMENT
FOR MANAGED SECURITY SERVICES

This Service Attachment is between Parker Data & Voice, LLC, a Texas company (sometimes referred to as "we," "us," "our," OR "Provider"), and the Client found on the applicable Order (sometimes referred to as "you," "your," OR "Client") and, together with the Order and relevant Service Attachments forms the Agreement between the parties.

The parties further agree as follows:

Provider will deliver to Client the IT infrastructure monitoring and management Services listed below and specifically identified on the Order and subsequent Order revisions, additions or changes. Unless otherwise indicated, Provider will deliver the Services on an ongoing basis.

Standard Security Services

- **Security assessment and report card (RAPID FIRE TOOLS)**
  Provider periodically will conduct information systems security testing procedures to evaluate the stability and security of Client's network, and Provider will deliver a written report identifying areas for concern or improvement.

- **Dark Web Monitoring (BREACH SECURE NOW OR CONTINUUM)**
  Provider periodically will deploy sophisticated Dark Web intelligence with search capabilities to identify, analyze and proactively monitor for an organization's compromised or stolen employee and customer data. Reports will be delivered periodically.

- **Next generation firewall Equipment and Software (WATCHGUARD FIREWALL W/TOTAL SECURITY)**
  Provider will deliver, deploy, configure and manage one or more compatible firewall devices – including associated firewall security software – on Client's network for Client's internal business purposes.

  The Service includes the following:
  - Installation and configuration of firewall traffic policies.
  - Apply updated firmware when applicable
  - Configuration changes when needed
  - Software services included on firewall:
  - Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows
  - URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content
  - Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses
  - Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk
  - Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.
  - Spam Prevention - Real-time, continuous, and highly reliable protection from spam and phishing attempts
  - Application Control – Provides the ability to allow, block, or restrict access to applications based on a user's department, job function, and time of day
  - APT Blocker - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.
  - Data Loss Prevention – works to enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP.
  - Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.
  - Intelligent Antivirus – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.
  - DNS Filtering - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

- **Centrally managed anti-virus Software (SENTINELONE)**
  Provider will acquire and will assign an appropriate number of licenses to support the deployment of an anti-virus software solution on devices covered under this Service Attachment.

  The Service includes the following:
  - Installation and application upgrades of antivirus software.
  - Real time virus scanning on all devices

- **Centrally managed Patch Management** (CONTINUUM RMM)
  Provider will acquire and will assign an appropriate number of licenses to support the deployment of a Windows Patch Management solution on devices covered under this Service Attachment.

  The Service includes the following:
  - Testing and deployment of Microsoft Security Patches within 5 days of release.
  - Testing and deployment of 3rd Party Security Patches when available.

Client-Side DNS Filtering (WATCHGUARD DNSGO OR WEBROOT DNS)
Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems.

The Service includes the following:
- Detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

SERVICE ATTACHMENT
FOR MANAGED SECURITY SERVICES

- Protects laptops while away from the corporate network.

Security Awareness Training & Phishing Simulations (BREACH SECURE NOW)
Provider will acquire and will assign an appropriate number of licenses to support the client environment.

The Service includes the following:
- Scheduled phishing campaigns to send at random times during a specified period.
- Trackable, fully customizable training course campaigns. Keep track of every user's participation, making all cybersecurity education accountable and measurable.
- Full catalog of cybersecurity and compliance training courses.

Multi-Factor Authentication Services (MICROSOFT MFA, AUTHY)
- Two factor authentications for compatible software applications.
- Single Sign on services for compatible software applications

- **Customized Security Policies and Procedures**
  After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider.

- **Quarterly Reporting, Reviews and Planning**
  Provider will deliver IT reporting and consulting services to assist Client in the holistic management of its IT environment. This service includes the following:
  - Technology impact assessment
  - Technology Compliance Assistance (SOX | PCI | HIPAA)
  - Technology Deployment Summary
  - IT Budget Planning
  - Documentation of Technology Environment
  - Network Performance Review

Premium Security Services
If Client has selected the Premium Service level, then in addition to all services included at the Standard Service levels, Provider will deliver the following:

- **Advanced Malware Protection supported by Security Operations Center (SENTINELONE OR THREATLOCKER)**
  - Deployment of advanced malware protection applications to all Windows based devices on customer network.
  - 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
  - Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings
  - Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state

- **Security Incident Event Management (SIEM) Services supported by SOC**
  - Deployment of SIEM monitoring probes to monitor all critical network devices including domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well.
  - Log monitoring and management - monitor key log files to identify and correlate events that could be malicious, while providing additional security and adherence to regulatory guidelines
  - Reporting for compliance requirements - generate daily reports and threat analysis outlines for three regulatory standards: HIPAA, PCI and NIST-800
  - SOC expertise and assistance

Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify the charges to apply for such assistance.

SUPPORT SERVICES

Coverage
Provider shall provide remote help desk and vendor management services through remote means between the hours of 8:00 am – 5:00 pm (U.S. Central time) Monday through Friday, excluding public holidays ("Normal Working Hours").

Support Outside Normal Working Hours
Upon request, Provider shall perform emergency Services outside of Normal Working Hours at the rates and according to the guidelines specified in the Order.

Maintenance Windows
Unless otherwise agreed, daily maintenance windows will be from 8:00 AM to 5:00 PM (U.S. Local time). Routine server and application maintenance and upgrades will occur during maintenance windows, and some applications, systems or devices may be unavailable or non-responsive during such times.

CLIENT ENVIRONMENT STANDARDS

In order for Client's existing environment to qualify for Provider's Services, the following requirements must be met:
- All servers with Microsoft Windows Operating Systems must be running current version of Windows Server supported by Microsoft and have all of the latest Microsoft Service Packs and

SERVICE ATTACHMENT
FOR MANAGED SECURITY SERVICES

Critical Updates installed and be patched within 30 days of the last patch.
- All desktop PC's and notebooks/laptops with Microsoft Windows Operating Systems must be running current version of Windows and have all of the latest Microsoft Service Packs and Critical Updates installed and be patched within 30 days of the last patch.
- All server and desktop software must be genuine, licensed and vendor supported.
- All wireless data traffic in the environment must be securely encrypted.
- Provider may deliver on-site Equipment in order to meet service requirements, as needed.
- Client's network environment must be configured with centralized authentication services such as Microsoft Active Directory or Radius services.

Healthcare Clients
- MS Active Directory

PCI-DSS (credit card)
- Segregated payment network
- Segregated wireless network from payment network
- MS Active Directory

All costs required to bring Client's environment up to these minimum standards are not included in this Service Attachment.

If Client's environment fails to satisfy the above requirements at any time during the Service term, Provider may suspend further delivery of the Services and/or terminate this Service Attachment upon five (5) business days' advance, written notice.

IF CLIENT CHOOSES A BACKUP SOLUTION THAT PROVIDER DOES NOT SUPPORT OR RECOMMEND, PROVIDER WILL MAKE BEST EFFORTS TO MONITOR SOLUTION FOR BACKUPS, BUT PROVIDER CANNOT GUARANTEE ANY OUTCOMES. CLIENT SHALL BE SOLELY RESPONSIBLE FOR ANY RESULTING OUTCOMES FOR NOT USING PROVIDER'S SUGGESTED OR RECOMMENDED BACKUP SOLUTION.

ADDITIONAL CLIENT OBLIGATIONS

Minor On-Site Tasks
Provider may occasionally request Client staff to perform simple on-site tasks. Client shall comply with all reasonable requests.

Server Upgrades or Repair
Provider will authorize the conduct of all server upgrades or repair. Client shall not perform any of these actions without Provider notification.

Security and Regulatory Recommendations
Although it is under no obligation to do so, from time to time, Provider may make recommendations regarding regulatory compliance, safety and security related to Client's network and practices (e.g., multi-factored authentication). If Client fails to adopt or implement the recommended protocols, Client is responsible for any and all damages related to regulatory, security, privacy, or data protection, including but not limited to fines, data breach notification, malware or ransomware costs, restoration, forensic investigation, restoring backups, or any other costs or damages related to Client's refusal to implement the recommended protocols.

NETWORK CHANGE COORDINATION

Significant Changes to Client's Network
Client shall notify Provider via email of all significant proposed network changes and shall provide the opportunity for Provider to comment and follow-up.

Research Regarding Network Changes
Evaluation of network change requests will sometimes require significant research, design, and testing by Provider. These types of requests are not covered by this agreement and will be billed at Provider's then-current rate for time and materials.

SERVICE FEES

Service Fees
For the Services described in this Service Attachment selected or ordered by Client, Client shall pay the Service Fees specified in the Order that is in effect at that time.

Client Delay
If Provider is unable to commence delivery of the Services on the Managed Services Start Date (defined below) because of any failure on the part of Client (including but not limited to failure of Client to provide the Client resources in a timely manner), Client nonetheless will begin to incur and Service Fees, which Client shall pay in accordance with this Service Attachment, beginning on the Managed Services Start Date.

EXCLUSIONS
Provider is not responsible for failures to provide Services that are caused by the existence of any of the following conditions or otherwise that occur during any period of time in which any of the following conditions exist:

Aged Hardware
Hardware which is no longer under either a manufacturer or third-party extended warranty covering hardware problems.

Problems Resulting from Client Hardware Malfunction
There is a defect or malfunction in any hardware or software that adversely affects Provider's ability to perform the Services.

Client Resource Problems
There are problems resulting from Client resources not under Provider management.

Client Personnel Problems
Provider's ability to resolve issues is due to problems with Client's personnel not under Provider's control.

Scheduled Maintenance
Scheduled maintenance windows and other agreed upon periods of time that are necessary for repairs or maintenance.

Network Changes
Changes made by Client to the networking environment that were not communicated to or approved by Provider.

Parker Data & Voice, LLC
Technology For Your Business

SERVICE ATTACHMENT
FOR MANAGED SECURITY SERVICES

Task Reprioritization
Problems or failures related to a prioritization or reprioritization of tasks by Client.

Force Majeure
Problems resulting from a Force Majeure Event as described in the Master Services Agreement.

Agreed Temporary Exclusions
Any temporary exclusion requested by Provider and approved by Client to implement changes in applications, environments, conversions or system software.

Client Actions
Problems resulting from actions or inactions of Client contrary to Provider's reasonable recommendations.

Client Responsibilities
Problems resulting from any failure by Client to fulfill its responsibilities or obligations.

Client Resolution
Provider's ability to resolve problems due to Client re-prioritizing Provider's recommendations.

Factors Beyond Provider's Control
Delays or downtime due to any factor outside of Provider's reasonable control.

Internet Connectivity Loss or Loss of Power
Loss of Internet connectivity to Client site for any reason.

Problem Ticket Management
The time interval between the initial occurrence of a desktop malfunction or other issue affecting functionality and the time Client reports the desktop malfunction or issue to Provider.

Third-Party Criminal Activity
Provider is not responsible for criminal acts of third parties, including but not limited to hackers, phishers, crypto-locker, and any network environment subject to ransom. You agree to pay ransom or hold provider harmless for any activity effecting network security on your environment related to third-party criminal activity. Any costs or fees to rebuild or service machines are provided and sold separately by Provider.

Viruses
Provider is not responsible for any harm that may be cause by Client's access to third party application programming interfaces or the execution or transmission of malicious code or similar occurrences, including without limitation, disabling devices, drop dead devices, time bombs, trap doors, Trojan horses, worms, viruses and similar mechanisms. Any costs or fees to rebuild or service machines are provided and sold separately by Provider.

Hardware Equipment
Client equipment must be maintained under manufactures warranty or maintenance contract or is in working order. Provider is not responsible for client equipment that is not maintained under manufacturer's warranty or maintenance contract or that is otherwise out of order. All fees, warranties, and liabilities against Provider assumes equipment is under manufactures warranty or maintenance contracts or is in working order.

TERM AND TERMINATION

Term
This Service Attachment is effective on the date specified on the Order (the "Service Start Date"). Unless properly terminated by either party, this agreement will remain in effect through the end of the term specified on the Order (the "Initial Term").

Renewal
"Renewal" means the extension of any Initial Term specified on a Order for an additional twelve (12) month period following the expiration of the Initial Term, or in the case of a subsequent Renewal, a Renewal term. This Service Attachment will renew automatically upon the expiration of the Initial Term or a Renewal term unless one party provides written notice to the other party of its intent to terminate at least sixty (60) days prior to the expiration of the Initial Term or of the then-current Renewal term.

Month-to-Month Services
If the Order specifies no Initial Term with respect to any or all Services, then we will deliver those Services on a month-to-month basis. We will continue to do so until one party provides written notice to the other party of its intent to terminate those Services, in which case we will cease delivering those Services at the end of the calendar month in which such written notice is received by the other party.

Early Termination by Client with Cause
If an Initial Term is specified in the Order, then you may terminate this agreement for cause following sixty (60) days' advance, written notice delivered to Provider upon the occurrence of any of the following:

- We fail to fulfill in any material respect our obligations under this agreement and fail to cure such failure within thirty (30) days following our receipt of your written notice.
- We terminate or suspend our business operations (unless succeeded by a permitted assignee under this agreement)

Early Termination by Client Without Cause
If an Initial Term is specified in the Order , and if you have satisfied all of your obligations under this Service Attachment, then no sooner than ninety (90) days following the Service Start Date, you may terminate this Service Attachment without cause during the Initial Term upon sixty (60) days' advance, written notice, provided that you pay us a termination fee equal to fifty percent (50%) of the recurring, Monthly Service Fees remaining to be paid from the effective termination date through the end of the Initial Term, based on the prices identified on the Order .

You may terminate this Service Attachment without cause following the Initial Term during any Renewal term upon sixty (60) days' advance, written notice, without paying an early termination fee.

Termination by Provider
We may elect to terminate this Service Attachment upon ninety (90) days' advance, written notice, with or without cause.

Parker Data & Voice, LLC
Technology For Your Business

SERVICE ATTACHMENT
FOR MANAGED SECURITY SERVICES

Effect of Termination

As long as Client is current with payment of: (i) the Fees under this Agreement, (ii) the Fees under any Project Services Attachment or Statement of Work for Off-Boarding, and/or (iii) the Termination Fee prior to transitioning the Services away from Provider's control, then if either party terminates this Service Attachment, Provider shall assist Client in the orderly termination of services, including timely transfer of the services to another designated provider. Client shall pay Provider at our then prevailing rates for any such assistance. Termination of this Service Attachment for any reason by either party immediately nullifies all access to Services supplied by Provider. Provider will immediately uninstall any affected software from your Client's devices, and Client hereby consents to such uninstall procedures.

Upon request by Client, Provider may provide Client a copy of Client Data in exchange for a data-copy fee invoiced at Provider's then prevailing rates, not including the cost of any media used to store the data. After thirty (30) days following termination of this Agreement by either party for any reason, Provider shall have no obligation to maintain or provide any Client Data and shall thereafter, unless legally prohibited, delete all Client Data on its systems or otherwise in its possession or under its control.

Provider may audit Client regarding any third-party services. Provider may increase any Fees for Off-boarding that are passed to the Provider for those third-party services Client used or purchased while using the Service.

Client agrees that upon Termination or Off-Boarding, Client shall pay all remaining third-party service fees and any additional third-party termination fees.

The remainder of this page is intentionally left blank.