MANAGED FIREWALL TERMS AND CONDITIONS

Blackfoot Communications' Managed Firewall Service (the "Service") is provided to the customer ("Customer") by Blackfoot Communications, Inc., dba Blackfoot Communications ("Blackfoot Communications"), (collectively, "Parties") pursuant to the terms and conditions of Customer's signed Service Order for the Service and the Master Service Agreement, which are incorporated herein, and these Managed Firewall Terms and Conditions ("Firewall Terms").

***IMPORTANT ***

MANAGED FIREWALL SERVICE IS FOR BUSINESS CUSTOMERS ONLY AND WILL BE MANAGED BY BLACKFOOT COMMUNICATIONS ON BEHALF OF CUSTOMER

In relation to the Service, the Parties agree:

1. SERVICE DESCRIPTION

1.1 The Service includes, at Customer's option and as reflected on Customer's fully executed Service Order, one or more of the following services, which services are described in more specificity in **§3** below:

1.1.1 Basic Services: Managed Firewall

1.1.2 Advanced Services: Managed Firewall; and/or

1.1.3 Optional Services: Enhanced Firewall Management Services (additional fees apply).

1.2 The Service is for business customers and is managed for Customer by Blackfoot Communications. The Service endeavors to thwart unwanted and malicious traffic from entering or leaving the firewall. Specifically, the Service provides Customers with firewall solution specification, configuration, installation, administration, monitoring, reporting, and support—as detailed in these Firewall Terms.

1.3 With this Service, Blackfoot Communications may sell Customer third-party firewall equipment and associated support packages. Except as otherwise agreed in a separate writing signed by the Parties, Customer shall purchase the third-party equipment via payment of a non-recurring charge at the inception of the Term. Blackfoot Communications may also take over the management of Customer's existing firewall equipment if that equipment was manufactured by Vendor and the type of equipment that Blackfoot Communications currently supports. If Blackfoot Communications takes over the management of Customer's existing firewall equipment, it will be reflected on Customer's Service Order.

2. DEFINITIONS

2.1 Unless otherwise designated in this agreement, capitalized terms shall have the same meaning as set forth in the Terms and the following words and phrases have the following meaning:

2.1.1 "Appliance(s)" shall mean the customer premise equipment (CPE) upon which the **Service** is configured.

2.1.2 "Blackfoot Communications Data Network" shall mean any Blackfoot Communications owned and operated Data Protocol (IP) routing infrastructure consisting of network-to-network interfaces (NNIs) and selected Blackfoot Communications POPs and the connections between them in the United States. The Blackfoot Communications Data Network does not include: (i) Customer premise equipment; (ii) any local loop or access facilities connecting Customer's premises to the Blackfoot Communications NNI if not owned by Blackfoot Communications; (iii) interconnections with other data service providers, (iv) other data service provider networks, or (v) other ISP networks beyond peering points for traffic routing.

2.1.3 "Firewall" shall mean a set of related programs and equipment that is designed to allow or deny certain hosts or networks to speak to each other, based on defined security policies.

2.1.4 "Manage(s)(d)(ment)" shall mean any Blackfoot Communications installs, configures and supports Customer hardware and software, pursuant to these Terms.

2.1.5 "Master Service Agreement" shall mean the Master Service Agreement attached to Customer's signed Service Order or if Customer orders the **Service** using Blackfoot Communications' online order process, then the Master Service Agreement located on Blackfoot Communication's website at http://www.blackfootcommunications.com/service-agreements/.

2.1.6 "MRC (Monthly Recurring Charge)" shall mean that each month during the Term Customer must pay Blackfoot Communications the MRC for the Service, as reflected on Customer's monthly invoice related to the Service.

2.1.7 "Near-net" shall mean a third-parity circuit (e.g. a circuit that is not owned by Blackfoot Communications) that is connected to Blackfoot Communications Data Network at a peering point.

2.1.8 "Off-net" shall mean a third-party circuit that does not connect directly to Blackfoot Communications Data Network.

2.1.9 "On-net" shall mean a circuit which is on Blackfoot Communications Data Network.

2.1.10 "QoS (Quality of Service)" shall mean the prioritization of certain types of Customer's network traffic over others to increase performance at Customer's request. QoS includes managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network to optimize network performance for Customer.

2.1.11 "SD-WAN Equipment" shall mean any hardware and software that provides a centralized WAN control function and allows Customer's service locations to leverage multiple data transport services (i.e. Broadband Internet, LTE, MPLS).

2.1.12 "Service Order" shall mean, as applicable, the Service Quote for the **Service** signed (a) physically by Customer along with the Master Service Agreement that accompanies it and the applicable exhibits and documents referenced therein, or (b) electronically by Customer using Blackfoot Communications' online order process along with Blackfoot Communications' then-existing Master Service Agreement located on Blackfoot Communications' website at http://www.blackfootcommunications.com/service-agreements/ and the applicable exhibits and documents referenced therein.

2.1.13 "Term" shall mean the duration of the Parties' Agreement related to the Service, as reflected on Customer's Service Order related to the Service.

2.1.14 "Vendor(s)" shall mean Blackfoot Communications' then-existing supported vendors associated with the **Service**, including but not limited to Vendor means

2.1.15 "WAN (Wide Area Network)" shall mean a telecommunications network that extends over a large geographic distance and that interconnects multiple local area networks.

3. SERVICE DESCRIPTION

3.1 Basic Services: Managed Firewall. Customers that order the Basic Services Managed Firewall from Blackfoot Communications shall receive the following services:

3.1.1 Service assessment, specification, configuration and installation.

3.1.1.1 Prior to the Installation Date Blackfoot Communications will work with Customer to help define security policies, QoS requirements, and verify the operation of the firewall equipment.

3.1.1.2 For firewall equipment purchased through Blackfoot Communications, configuration and policy setting will take place at Blackfoot Communications' facilities unless agreed otherwise in a writing signed by the Parties. For Customer-provided firewall equipment, Customer will have the option to (i) ship the firewall equipment to Blackfoot Communications to configure at Blackfoot Communications' facilities, or (ii) require a Blackfoot Communications technician to configure the equipment at Customer's location, in which case Customer shall pay Blackfoot Communications' travel-related expenses and Blackfoot Communications' then-existing labor and material fees associated with the Blackfoot Communications technician(s).

3.1.1.3 Neither physical installation of equipment nor the extension of cabling from the firewall to either the LAN (Local Area Network) or WAN is provided as part of the Service unless these services are listed on Customer's fully executed Service Order.

3.1.1.4 When taking over management of an existing firewall, Blackfoot Communications will typically perform the configuration remotely. Customer may be required to physically load media on its systems. All managed firewalls will require some remote configuration.

3.1.2 Administration and Support.

3.1.2.1 Included with the Service is one (1) change event per month—whether it be a single change or a group of multiple requested configuration changes at the same time—up to a maximum of one (1) hour of labor time. Labor time in excess of one (1) hour will be billed at Blackfoot Communications' then-existing hourly rates. Except as provided in **§3.1.3.3** below, Blackfoot Communications will make the changes during Blackfoot Communications' normal business hours.

3.1.2.2 Blackfoot Communications will acknowledge receipt of the Customer's policy change request: (i) immediately if the Customer's request is made via phone, and (ii) within four (4) business hours of receipt if the request is made by email during normal Blackfoot Communications' normal business hours—e.g. 8am-5pm MST. This guarantee is only available for policy change requests submitted by a Customer's IT contact who is identified on the Authorized on Account ("AOA") form Customer executes and delivers to Blackfoot Communications.

3.1.2.3 Customer acknowledges and agrees Customer is solely responsible for all matters relating to Customer's network security, including but not limited to developing, defining, and carrying out policies, plans, and procedures relating to Customer's network security, cyber security, incident and breach response. While Customer is solely responsible for deciding a firewall's policy and configuration, Customer acknowledges and agrees Blackfoot Communications alone will make the Customer-decided changes to a firewall's policy and/or configuration; Customer will not make those changes.

3.1.2.4 On an annual basis, Blackfoot Communications will audit Customer's policy settings based upon (i) a baseline document of Customer-elected policy settings created following the consultation referenced in **§3.1.1** above, and (ii) Customer-initiated policy change requests.

3.1.2.5 To obtain support Customer (i) may call Blackfoot Communications Business Technical Support directly at 406-541-5072 and, as backup, may call Blackfoot Communications' main switchboard at 866-541-5000 (Customer should request Business Technical Support), or (ii) may email Blackfoot Communications Business Technical Support at tac@blackfoot.com;

3.1.3 Troubleshooting and Resolution.

3.1.3.1 Firewall. If the firewall is identified as the potential source of a network-related problem, Blackfoot Communications will examine the device configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by Blackfoot Communications, or an active troubleshooting session between Blackfoot Communications and Customer. Blackfoot Communications will endeavor to resolve technical issues as expediently as feasible. If the firewall is eliminated as the source of a given problem, Blackfoot Communications will perform no further troubleshooting. Service includes troubleshooting and resolution during Blackfoot Communications' normal business hours. Blackfoot Communications will work to address and implement Customer change requests within a 24-hour period during Blackfoot Communications' normal business week. Some request are more complex and the completion timeframe depends upon the scope of the changes and the Customers' requirements for service windows.

3.1.3.2 No network downtime is considered to have occurred if one or more circuits at the affected service site is able to transmit and receive data.

3.1.3.3 Emergency change requests. Blackfoot Communications will prioritize Customer emergency change requests over routine change requests when requests are made via the designated Blackfoot Communications telephone contacts noted above in **§3.1.2.5.** An emergency change request is a request related to a security breach or person or entity reaching a portion of Customer's network the Customer is not authorized to access, and not a routine change request. Blackfoot Communications' prioritization of Customer's emergency change requests is only available for requests submitted by a valid Customer contact as identified on the Customer's AOA form.

3.1.3.4 After-hours support. Support is available to Customer at Blackfoot Communications' then-existing after-hours support rates, subject to a minimum charge for 2 hours of technician time (a 2 hours minimum is required for an on-call technician to establish a secure computer log in, review network monitoring information, make an assessment, contact Customer, and complete resolution in consultation with the Customer.) Customer LAN support is not included in the 2-hour minimum charge but can be provided subject to Blackfoot Communications' then-existing after-hours support rates.

3.1.4 Software Upgrades.

3.1.4.1 Not all Vendor software updates are routinely applied.

3.1.4.2 Blackfoot Communications will check for a firewall operating system (OS) upgrade to the Vendor-recommended version and apply the upgrade if a newer "Safe Harbor" or equivalent version is needed at least one (1) time per year (Cisco defines "Safe Harbor" as "Safe Harbor certification marks the successful completion of extensive integrity testing that validates each release."). Certain firewall solutions may be cloud-based and are updated automatically by the Vendor without Blackfoot Communications' intervention.

3.1.4.3 Customer and Blackfoot Communications will coordinate for appropriate scheduling. The after-hour support rules in **§3.1.3.3** above apply here as well.

3.1.4.4 Should Vendor provide a notification to Blackfoot Communications of a software bug or a new threat update requiring immediate application to Customer's firewall, Blackfoot Communications will apply such Vendor OS upgrade to address the issue(s).

3.1.5 Configuration Backup and Recovery.

3.1.5.1 Blackfoot Communications automatically archives the most recent configuration of the Customer's firewall for backup and restore purposes once per week. Certain firewall solutions may be cloud-based and are backed-up automatically by the Vendor to the Vendor's location and without Blackfoot Communications intervention. Customer agrees Blackfoot shall have no responsibility or liability associated with backups.

3.1.5.2 Backups are also captured as changes are made to Customer's firewall.

3.1.5.3 Blackfoot Communications replicates backups to an offsite location.

3.1.5.4 In case of hardware failure, or a lost or corrupted configuration, Blackfoot Communications treats the issue as a high priority and endeavors to work promptly with Customer and the applicable Vendor to address the issue. The third-party hardware leased to Customer shall be replaced or repaired, if at all, pursuant to the warranty terms and conditions of the Vendor that sold such equipment to Blackfoot Communications. If Customer requests to have such third-party hardware repaired or replaced during the 12 months preceding the end of the Term, then before Blackfoot Communications is obligated to repair or replace that equipment (assuming it is required under Vendor's warranty) Customer must sign a new Service Order for **the Service** with a minimum term of thirty-six (36) months.

3.1.5.5 Blackfoot Communications will replace the third-party equipment leased to Customer that is lost stolen or damaged where replacement is not covered under Vendor's warranty in which case Blackfoot Communications will charge Customer, and Customer agrees to pay, a replacement fee, which replacement fee will be the lesser of (i) $500, and (ii) twenty-five percent (25%) of the sum of the remaining monthly recurring charges in the Term for **the Service.**

3.1.5.6 The after-hours support rules in §3.1.3.4 above apply here as well.

3.1.6 Site-to-Site VPN (Virtual Private Network).

3.1.6.1 Blackfoot Communications will manage a Customer's site-to-site VPN for a Customer when Blackfoot Communications manages all of that Customer's VPN end point.

3.1.6.2 If third party interworking is required (e.g., VPN end point is not managed by Blackfoot Communications), additional charges based on Blackfoot Communications' then-existing labor and material charges may apply (e.g. including but not limited to troubleshooting with 3rd party IT vendor, Customer, or supporting non industry standard protocols or practices.).

3.1.7 Support for up to five (5) zones (WAN, LAN, DMZ, WLAN, Security).

3.1.7.1 Blackfoot Communications will segregate up to five (5) zones from each other on Customer's firewall.

3.1.7.2 Blackfoot Communications will provide ongoing support for zone changes requested by Customer pursuant to the support rules outlined in **§§3.1.2-3.1.3** above.

3.2 Advanced Services: Managed Firewall

3.2.1 In addition to the services described in **§3.1** above, Customers who order the Advanced Services Managed Firewall from Blackfoot Communications shall select the services to receive from **§3.2** below. All of the features in Advanced Services Managed Firewall require additional licensing and labor, some require additional hardware, and if Customer selects a service from **§3.2,** the service will be shown on Customer's Service Order related to the Service.

3.2.1.1 Security Policies and Configuration Features. Following successful deployment of the Managed Firewall – Advanced service, Customers may submit requests to modify the configuration of Customer's selected features below by submitting a policy change request, subject to the terms and conditions outlined in **§§3.1.2-3.1.3** above.

3.2.1.2 Application Visibility and Control.

3.2.1.2.1 A suite of service application level monitoring, classification and traffic control options is available.

3.2.1.2.2 During the initial Customer configuration requirements discussion(s), or at a later date per **§3.1.2** above, Blackfoot Communications can help optimize network performance and help define policies for each of the Customer applications utilizing the network. This includes but is not limited to de-prioritizing or blocking competing non-critical traffic (e.g., Pandora, Facebook, etc.).

3.2.1.3 Content Filtering (specific URL control).

3.2.1.3.1 Content filtering is designed to address the concerns of Customer that wish to leverage the benefits of Internet Web access, yet are concerned about the possible loss of productivity and potential of encountering objectionable Internet content.

3.2.1.3.2 Below is a general overview of features within the content filtering tool:

3.2.1.3.2.1 Category Lists - a selection of content categories to block (i.e.: gambling, adult content, games, and social media).

3.2.1.3.2.2 Destination White Lists - specific sites that should be allowed even if they exist within a denied content category.

3.2.1.3.2.3 Destination Black Lists - specific sites that should be blocked even if they exist within an allowed content category.

3.2.1.3.2.4 Source White List - specific IP addresses that should be excluded from content filtering.

3.2.1.3.3 Web search filtering, including images.

3.2.1.4 IDS (Intrusion Detection System) and IPS (Intrusion Prevention Service).

3.2.1.4.1 IDS and IPS are tools intended to detect and prevent intrusions, internally and externally, in supported devices via rulesets: pre-defined security policies that determine the level of threat protection needed. There are three rulesets: Connectivity, Balanced, and Security, with defined threat metrics and criteria for each:

3.2.1.4.1.1 Connectivity ruleset. Intended to protect against the highest-priority threats discovered in the current year as well as the prior two (2) years.

3.2.1.4.1.2 Balanced ruleset. Intended to protect against vulnerabilities identified in the Connectivity ruleset, slightly less critical threats, and certain categories of threats (e.g. exploit kits and SQL injections) regardless of age.

3.2.1.4.1.3 Security ruleset. Intended to protect against vulnerabilities identified in the Connectivity and Balanced rulesets as well as lower-priority threats, but expands the age limit to vulnerabilities discovered within the last 4 years. Additionally, an expanded list of threat categories are intended to be caught, regardless of age.

3.2.1.5 Network Anti-Virus and Malware Protection. This service provides gateway detection of virus, botnet and malware threats.

3.2.1.6 Security Content Updates for IPS and AV/Malware. Blackfoot Communications will update security platforms with the most-current Security Content. As used in the Firewall Terms, Security Content means new checks or signatures for the Intrusion Prevention system, antispam and antivirus modules, and new URL listings for the Web filtering module. Such Security Content enhances the firewall's security capabilities. At Blackfoot Communications' discretion, Security Content updates may be downloaded and installed onto the security platform at any time. Such an operation is transparent to users.

3.2.1.7 File Filtering. File type blocking and inspection (e.g., .exe, macros).

3.2.1.8 Advanced Threat Alerting. There are a number of options available for email alerts to be sent when certain network or device events occur. Customer may choose which alerts to enable, including but not limited to: VPN connection state (up/down), configuration changes, up/down status of the security appliance, link state changes or if failover occurs in high availability configurations.

3.3 Enhanced Services: Firewall Management Services. The following services are available to Customer on an a la carte basis, for an additional fee. Upon request, Blackfoot Communications will provide Customer a quote for one or more of these Optional Firewall Management Services. Blackfoot Communications shall not be obligated to provide the Optional Firewall Management Services until the Parties have executed a Service Order related to the Optional Firewall Management Services requested by Customer.

3.3.1 4G LTE Failover. The 4G LTE Failover service provides Customer with the configuration and delivery of hardware and software relating to a 4G LTE failover network connection. Customer shall receive up to 1 Gigabyte of 4G LTE failover each month during the Term; however, Customer shall pay Blackfoot Communications a fee for each additional gigabyte of 4G LTE failover used in excess of the baseline 1 Gigabyte of 4G LTE failover that is provided per month with this service.

3.3.2 High Availability Service.

3.3.2.1 The High Availability ("HA") service increases the reliability of the Service by supporting the implementation of redundant firewall devices into Customer's managed environment. Adding HA to the Service may require changes to the firewall platform, software licensing, IP addressing requirements, and/or managed service fees. The Service does not support non-integrated, third party HA solutions.

3.3.2.2 Upon request, Blackfoot Communications may quote Customer a HA configuration and include it in the Service if the Parties sign a Service Order for the HA service. The HA option helps protect against hardware failure. Under this option, two managed firewalls may be configured and deployed—one fully operational, and the other serving as a backup firewall should the first firewall fail. Some firewalls can also be deployed as clusters, such that both firewalls operate and share network load.

3.3.3 Site-to-Site VPN using a Third Party End Point. Under this optional service Blackfoot Communications will configure Customer's Service to allow a VPN to be establish between Customer and a third party's VPN device ("VPN end point"). Unless Blackfoot Communications agrees to do so in a Service Order signed by the Parties, the third party's VPN device will not be provided or managed by Blackfoot Communications. Blackfoot Communications will provide Customer with the configuration information relating to Customers' Service needed for the third party to configure its VPN device accordingly. Blackfoot Communications makes no representation or warranty of any kind relating to non-Blackfoot Communications managed VPN end point ("Extranet VPN") and is not responsible for its security or functioning. Unless Blackfoot Communications agrees to do so in a separate signed writing, Blackfoot Communications will not manage, monitor, administer, report or support the Extranet VPN. Customer understands that a change to the Service may affect the Extranet VPN and that it is Customer's sole responsibility to make arrangement regarding the third party's VPN device to enable the Extranet VPN to function.

3.3.3 Customer VPN. The Customer VPN service allows remote users to securely access files and services on the Customer's network through an encrypted tunnel over the Internet.

3.3.3.1 This service is facilitated by use of a software client installed and/or setup on the user's local computer.

3.3.3.2 This service may require additional licensing and costs to setup and incorporate Customer VPN into the Customer's existing environment (i.e., Active Directory Authentication).

3.3.3.3 Blackfoot Communications will bill Customer for setup on end user's devices based on Blackfoot Communications' then-existing hourly rates, with a minimum charge of 30 minutes per device. Alternatively, Customer may install the Customer VPN.

3.3.3.4 In some cases, it may not be possible because of a remote networks design for a user to connect via VPN. If this is determined Blackfoot Communications will try alternative configurations, where appropriate, but functionality of the Customer VPN is not guaranteed.

3.3.4 SSL decryption (requires licensing, only available on ASA with Firepower).

3.3.4.1 SSL (Secure Sockets Layer) is an industry standard for transmitting secure data over the Internet.

3.3.4.2 SSL-encrypted traffic is decrypted, inspected by the Service, and then re-encrypted before it is sent to its original destination. This allows the standard IPS, Malware, File and Content Filtering to function as it would on non-encrypted traffic.

3.3.4.3 The service requires installation by Customer of a Certificate on all user machines inside the network.

3.3.4.4 The service requires that the public and private key pair be installed on the public facing server and the Cisco ASA.

3.3.5 On-site installation: On-site assistance at Customer's location by a Blackfoot Communications technician and/or network engineer is not included in the Service. Customer may request, and Blackfoot Communications will quote, the following: labor, travel, and materials. The scope of on-site installation services, and the fee for same, will be detailed in a separate Service Order signed by the Parties.

4. CUSTOMER REQUIREMENTS

4.1 Customer agrees to perform the following obligations and acknowledges and agrees Blackfoot Communications' ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

4.1.1 Hardware/Software Procurement. Except as otherwise provided in these Firewall Terms, Customer is responsible for purchasing the firewall hardware and software necessary for Blackfoot Communications to provide the Service. Additionally, Customer is responsible for ensuring that Customer's hardware and software stays within the versions supported by the Service. Blackfoot Communications' SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updated by the Vendor.

4.1.2 Support Contracts. Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned firewall and connectivity to prevent network performance degradation and for maintaining communications between the Customer's contracted firewall devices and Blackfoot Communications. Blackfoot Communications' SLAs will not apply if Customer does not abide by this obligation.

4.1.3 RMA (Return Materials Authorization) Responsibilities. If Customer grants Blackfoot Communications exclusive access to the Vendor support account pursuant to **§ 6.3** below Blackfoot Communications is responsible for initiating the Return Materials Authorization ("RMA") process; in all other cases Customer is responsible for same. Customer is, however, responsible for fulfilling the RMA process directly with Vendor in the event that the hardware and/or software managed by Blackfoot Communications is determined to be in a failed or faulty state and requires replacement.

4.1.4 Connectivity. Customer will provide access to Customer-premises and relevant appliance(s) necessary for Blackfoot Communications to manage and monitor the contracted firewall devices. Additionally, Customer shall communicate to Blackfoot Communications any network or system changes that could impact Service via the process in **§3.1.2.5** above. Service activation that may require device downtime will depend on customer deliverables such as on-site assistance with initial configuration of the appliance to get connectivity. SLAs will not apply to devices that are experiencing Customer-caused or non-Blackfoot Communications caused connectivity issues.

5. SERVICE LEVELS

SERVICE	STANDARD SLA	SLA CREDIT
Standard Change Request **§3.1.2.1 – 3.1.2.2**	Acknowledgment by Blackfoot Communications of its receipt of Customer's Change Request within four business hours during normal	1/30th of the MRC of the impacted Service

	business hours (e.g. 8am-5pm MST) of Blackfoot Communications' receipt of the Change Request.	
Troubleshooting and Resolution **§3.1.3**	Acknowledgment by Blackfoot Communications of its receipt of Customer's notification of a technical issue within four business hours during normal business hours (e.g. 8am-5pm MST) of Blackfoot Communications' receipt of the notification.	1/30th of the MRC of the impacted Service
Annual Software Update (Cisco ASA series firewalls only) **§3.1.4.2**	Customer shall receive a Safe Harbor update up to once per year.	1/30th of the MRC of the impacted Service
Configuration Backup and Recovery (Cisco ASA series firewalls only) **§3.1.5**	Customer will receive an archive of the most recent configuration of the Customer's firewall for backup and restore purposes once per week	1/30th of the MRC of the impacted Service
Annual Audit **§3.1.2.4**	Blackfoot Communications shall perform one audit of Customer firewall configuration per year.	1/30th of the MRC of the impacted Service

6. ADDITIONAL RULES, REGULATIONS, TERMS AND CONDITIONS

6.1 Configuration. Blackfoot Communications has Cisco and Cisco-Meraki certified network engineers who follow industry standards regarding configuration.

6.2 Secure Access. Blackfoot Communications technicians remotely access Customer's managed devices through a secure (encrypted) and restricted connection. Blackfoot Communications retains root access to Customer's firewall(s) managed hereunder during the Term.

6.3 Vendor Support Agreements. As a condition to receiving the Service, Customer must purchase appropriate Vendor support contracts for the duration of the Term. To enable Blackfoot Communications to fulfill its obligations relating to this Service, Customer shall provide Blackfoot Communications with exclusive access to the Vendor support account.

6.4 Transferrable Management. When Customer's contract with Blackfoot Communications relating to this Service expires or is terminated, Blackfoot Communications will leave intact the firewall configuration on the Customer-owned device(s), but remove (1) Blackfoot Communications' credentials for access to the Customer-owned device(s) and (2) Blackfoot Communications' proprietary firewall configuration—e.g., Blackfoot Communications' proprietary configuration would include but not be limited to passwords, logging to external servers, and any configuration that Blackfoot Communications has developed in-house that other providers do not offer. The Service does not include assistance in migrating Customer to another service provider.

6.5 Firewall Replacements and Upgrades. The Service includes configuration time applied by Blackfoot Communications to new and replacement Customer firewalls of the same Vendor family provided under the terms of the required Vendor support contact.

6.6 Support for most server and network device protocols. The Service includes and is limited to PING, HTTP, HTTPS, DNS, FTP, POP3, SMTP, IMAP, SSH, Telnet, My SQL, MS SQL, and Custom server and device protocols.

6.7 Project work. Changes constituting a Customer-initiated redesign are subject to Blackfoot Communications' current hourly rates. Customer-initiated redesign work includes but is not limited to significant firewall updates—e.g. updates that exceed the scope of **§3.1.2.1**, which without limitation can consist of changes by Customer's compliance requirements (e.g., PCI, , SOX, etc.) and/or other Customer-initiated audits or network changes.

6.8 Breach. Customer agrees to provide Blackfoot Communications with sufficient information, as determined by Blackfoot Communications, to allow Blackfoot Communications to configure the Services in a way that meets Customer's security needs, as those needs are decided solely by Customer. Should Blackfoot Communications determine that there has been unauthorized access to the firewall (a breach), Blackfoot Communications will notify Customer as soon as possible and Blackfoot Communications and Customer will work together to determine a course of action with regard to the breach. Customer hereby authorizes Blackfoot Communications take unilateral action, including but not limited to suspending all or part of the Services, to isolate and mitigate the cause of a breach. Blackfoot Communications' breach notification to Customer may contain preliminary and unconfirmed information; however, it is provided to Customer to assist in efforts to mitigate the effects of a breach. Blackfoot Communications and Customer each agree to reasonably cooperate with each other to investigate the facts and circumstances involved in a breach. To the extent Blackfoot Communications' cooperation requires time and resources above and beyond those extended by Blackfoot Communications in conjunction with a typical breach investigation, or should Blackfoot Communications be asked to cooperate with a governmental investigation, Customer will be billed at Blackfoot Communications' standard labor rates.

6.9 Takeovers. As a condition to Blackfoot Communications taking over management of an existing Customer firewall, Blackfoot Communications must assess the firewall to be sure it meets certain specifications. As a condition to providing Service in relation to an existing Customer firewall, Blackfoot Communications may require: (1) the firewall software to be upgraded to the most current versions; and (2) an active support contract be purchased by Customer from Vendor. Other required criteria may include but are not limited to the addition, modification and/or removal of applications and user accounts.

6.10 Off-Net Service Management. The Service may be utilized by Customer with third party circuits (off-net). The Service provides the same level of benefit on an off-net circuit as it does with on-net/near-net connected Service; however, Service may be limited by variables introduced by use of a third party network that are beyond Blackfoot Communications' reasonable ability to troubleshoot and control. Functions such as QoS will be limited due to the nature of third party (off-net) circuits and support times are reliant on third-party resolution. At Customer's option, Blackfoot Communications may quote, procure and rebill to Customer, on the monthly Blackfoot Communications billing statement, such third-party circuits.

6.11 NO GUARANTEE. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE SERVICES DOES NOT ACHIEVE THE IMPOSSIBLE GOAL OF RISK ELIMINATION, AND THEREFORE BLACKFOOT COMMUNICATION DOES NOT GUARANTEE THAT INTRUSIONS, COMPROMISES, OR OTHER UNAUTHORIZED ACTIVITY WILL NOT OCCUR ON CUSTOMER'S NETWORK.

6.12 Scheduled Maintenance Outages. Blackfoot Communications may schedule maintenance outages for Blackfoot-owned equipment/servers that are being utilized to perform the Service with one (1) weeks' notice to Customer's designated contacts.

6.13 Service Levels. The Service Levels set forth above are subject to the following terms, conditions, and limitations:

6.13.1 The Service Levels shall not apply during scheduled maintenance outages and therefore are not eligible for any Service Level credit. Blackfoot Communications shall not be held liable for

any Service impact or Service Levels Agreements related to configurations that are not supported by Blackfoot Communications.

6.13.2 The Service Levels shall not apply in the event of any Customer-caused service outage that prohibits or otherwise limits Blackfoot Communications from providing the Service, delivering the Service Levels or managed Service descriptions, including but not limited to: Customer misconduct, Customer negligence, inaccurate or incomplete information provided by the Customer, Customer modifications made to the Services, or any unauthorized modifications made to any managed hardware or software devices by the Customer, its employees, agents, or third parties acting on behalf of Customer.

6.13.3 The Service Levels shall not apply to the extent Customer does not fulfill and comply with the Customer obligations set forth in these Firewall Terms or the Service Order or Master Service Agreement between the Parties related to the Service. The obligation of Blackfoot Communications to meet the Service Levels with respect to any incident response or ticket request are conditioned upon Blackfoot Communications' ability to connect directly to the Customer devices on the Customer network through an authenticated server in Blackfoot Communications' operations center.

6.13.4 Customer will receive credit for any failure to meet the Service Levels outlined above within thirty (30) days of notification by Customer to Blackfoot Communications of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Blackfoot Communications within thirty (30) days of such failure. Blackfoot Communications will research the request and respond to Customer within thirty (30) days from the date Blackfoot Communications received the request.

6.13.5 The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the MRC paid by Customer for the impacted Service. The foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

6.14 **Reservation of Rights.** Blackfoot Communications reserves the right to modify these Firewall Terms, including the SLAs, in which case Blackfoot Communications will post the updated version of the Firewall Terms to Blackfoot Communications' website.