



MANAGED SECURE ACCESS SERVICE EDGE (SASE) TERMS AND CONDITIONS

Blackfoot Communications' Managed Secure Access Service Edge (the "Service"), commonly referred to as Managed SASE, is delivered by Cato Networks, Inc. ("Cato") provided to the customer ("Customer") by Blackfoot Telephone Cooperative, Inc., Blackfoot Communications, Inc., and Fremont Telcom Co., and their respective direct and indirect affiliates and subsidiaries, collectively doing business as Blackfoot Communications ("Blackfoot Communications") (collectively, the "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 Terms and Conditions ("Terms").

IMPORTANT

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

In relation to **MANAGED SASE**, the Parties agree:

1. OVERVIEW

1.1 The **Service**, SASE, is a managed solution that provides a secure overlay network to interconnect customer locations and the cloud with security elements. 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 Coordinated and planned configuration of cloud software by Cato that steers traffic based on business policy rules provided by, or set forth by the Customer;
- 1.1.2 Installation and configuration of SASE hardware at customer premises (referred to herein as "Socket") including hardware sparing and RMA coordination.
- 1.1.3 View-only and/or administrative access to a centralized management console;
- 1.1.4 Installation and management of network connections;

1.2 The **Service** is for business customers only and is managed for Customer by Blackfoot Communications at the Customer's direction. Blackfoot Communications, via the **Service**, endeavors to provide Customer with enhanced network performance, security and reliability.



1.3 With this **Service**, Blackfoot Communications may lease or sell Customer third-party equipment and associated third-party licensing/support packages. Blackfoot Communications may also take over the management of Customer's existing equipment if that equipment was manufactured by Vendor and is the type of equipment that Blackfoot Communications currently supports. If Blackfoot Communications takes over the management of Customer's existing equipment, it must be reflected in a Service Order signed by the Parties. Customer agrees that all Blackfoot Communications managing of Customer equipment is done at the sole direction of the Customer. The Customer retains full control over and liability for decisions associated with the Service.

1.4 Customer and Blackfoot Communications agree that this service is provided under a contract and is not statutory in nature.

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 "Manage(d)(ment)" shall mean Blackfoot Communications installs, configures and supports Customer SASE socket and software pursuant to these Managed SASE Terms and as reflected on Customer's monthly invoice related to the **Service**.

2.1.2 "MRC (Monthly Recurring Charge)" shall mean 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**.

2.1.3 "Near-net" shall mean a near-net circuit is a third-party circuit (e.g. a circuit that is not owned by Blackfoot Communications) that is connected to Blackfoot Communications' network at a peering point.

2.1.4 "Off-net" shall mean an off-net circuit is a third-party circuit that does not connect directly to Blackfoot Communications' network.

2.1.5 "On-net" shall mean an on-net circuit is on Blackfoot Communications' WAN.

2.1.6 "QoS" shall mean the Quality of Service, meaning prioritization of certain types of Customer's network traffic over Customer's other network traffic 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.

2.1.7 "Term" shall mean the Term is the duration of the Parties' agreement related to the **Service**, as reflected on Customer's Service Order related to the **Service**.

2.1.8 "Vendor(s)" shall mean Cato Networks (Cato).

2.1.9 "Socket" shall mean the customer premise equipment (CPE), physical or virtual, that securely connects branch offices and data centers to the Cato SASE Cloud.



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

2.1.11 “Authorized User”. Shall mean any employee, contractor, representative, or other person acting on Customer’s behalf who is authorized by Customer to use the Service and who has been supplied with access to the Service by either Customer or Blackfoot, at Customer’s written request. Customer is responsible for maintaining the status of its Authorized Users and for all the activity of such Authorized Users and their use of the Service.

3. SERVICE DESCRIPTION

3.1 Subscription Services. The Service is provided to Customer subject to the terms and conditions of this Agreement and during the Term. Customer’s Service Order will specify the authorized scope of use for the Service, which may include: (a) the bandwidth volume per site; (b) the number of remote users; and (c) other subscribed features such as Threat Prevention, Advanced Threat Prevention, Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP).

3.2 Standard Service Onboarding. As a separate non-recurring Professional Services charge, Blackfoot Communications shall provide project management and technical enablement services as required to implement and configure the Service and provision access to Customer’s authorized users. Standard service onboarding is offered during Blackfoot’s regular business hours. Custom service onboarding may be required for certain deployments, which must be agreed to between the parties in the statement of work.

3.3 Managed Service Levels. Blackfoot Communications offers two managed service levels: (i) SASE Managed Support and (ii) SASE Managed Support Advanced. Customers that order the Service shall receive the following services:

3.3.1 SASE Managed Support includes:

3.3.1.1 Coordinated and planned configuration changes requested by the Customer and approved by Blackfoot that are not part of the Standard Service Onboarding. Configuration and policy settings for the Service, as selected by Customer, will be performed by Blackfoot Communications, unless agreed otherwise in writing signed by the Parties.

3.3.1.2 Change requests at this support level do not include requests related to CASB or DLP.

3.3.1.3 Configuration change requests supported include TLS decryption adjustment, whitelist/blacklist for Internet, WAN, and LAN policies, ZTNA client connectivity and ZTNA policy updates (only for customers who have ZTNA included as part of the Service as reflected on signed Service Order).

3.3.1.4 Promptly upon Vendor announcement of security vulnerabilities, software/firmware updates are to be performed in coordination with Customer; otherwise, versions are reviewed quarterly with upgrades scheduled as needed.

3.3.2 SASE Managed Support Advanced includes:



3.3.2.1 In addition to the services provided in SASE Managed Support (3.3.1) SASE Managed Support Advanced includes CASB and DLP configuration changes requested by the Customer and approved by Blackfoot will be performed by Blackfoot Communications, unless agreed to otherwise in writing signed by the Parties.

3.4 **Add-On Services.** The service features below are available as add-ons and do not form a part of the Service unless reflected in a Service Order signed by the Parties.

3.4.1 Physical installation of socket or other customer premise equipment is not included as part of the Service, unless otherwise listed on Customer's fully executed Service Order.

3.4.2 If an extension of cabling from the circuit demarcation point(s) to the socket is required Blackfoot Communications will charge Customer a one-time extension fee to complete the cable extension, based on Blackfoot Communications' then-existing extension fees.

3.4.3 When taking over management of existing customer premise equipment, Blackfoot Communications will typically perform the configuration remotely. The Customer may be required to physically load media. All SASE appliances will require remote configuration.

3.5 **Administration and Support**

3.5.1 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.

3.5.2 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, and incident and breach response. While Customer is solely responsible for deciding on policy and configuration, Customer acknowledges and agrees Blackfoot Communications alone will make the Customer-directed changes to policy and/or configuration of the Service; Customer will not make those changes.

3.5.3 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
noc@blackfoot.com.

3.6 Troubleshooting and Resolution

- 3.6.1** 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.
- 3.6.2** 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 requests are more complex, and the completion timeframe depends upon the scope of the changes and the Customers' requirements for service windows.
- 3.6.3** 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 § 3.5.3. An emergency change request is a request related to a network outage or security breach, 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.
- 3.6.4** After-hours remote support. Remote 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.)

3.6.5 Software Upgrades

3.6.5.1 Not all Vendor software updates are routinely applied.

3.6.5.2 Customer acknowledges, understands, and agrees Blackfoot Communications will review the recommended software and/or firmware updates from the Vendor and coordinate with Customer to schedule recommended updates as needed. Blackfoot Communications will make all commercially reasonable efforts to gain Customer approval to implement such updates. Application of updates will be done at the sole direction of the customer. If the Customer does not upgrade, either through choice or error, Customer accepts liability for breaches experienced as a result.

3.6.5.3 Customer and Blackfoot Communications will coordinate for appropriate scheduling. The after-hour support rules in § 3.6.4 above apply here as well.



3.6.6 Configuration Backup and Recovery

3.6.6.1 The Service is cloud-based and is backed-up automatically by the Vendor to the Vendor's location and without Blackfoot Communications intervention.

3.6.6.2 In case of hardware failure, or a lost or corrupted configuration, Blackfoot Communications treats the issue as a high priority and endeavors to promptly resolve it for Customer with the Vendor.

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

3.6.7 Traffic-based Policy Management

3.6.7.1 Blackfoot Communications will make Customer decided policy configuration changes when requested by customer. Support rules in § 3.6.3 above apply here as well.

3.6.8 Security Monitoring and Mitigation

3.6.8.1 Blackfoot Communications does not provide monitoring for security events, any security event mitigation, or advice regarding security issues or threats. Upon request by Customer, Blackfoot Communications will modify the configuration of the Service in accordance with the specifications provided by Customer to attempt to mitigate security events and security threats identified by Customer. Blackfoot Communication's sole obligation is to implement the configuration settings requested by Customer. Blackfoot Communication's makes no guarantees with respect to the detection or blocking of viruses/worms/malware or any other type of attacks and is not responsible for any such malicious data that may be transmitted over the provided network.

3.7 Optional Services

3.7.1 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 Services. Blackfoot Communications shall not be obligated to provide the Optional Services until the Parties have executed a Service Order related to the Optional Services requested by Customer.

3.7.1.1 High Availability Service

3.7.1.1.1 The High Availability ("HA") service increases the reliability of the Service by supporting the implementation of redundant sockets into the Service. Adding HA to the Service may require changes to the software licensing, IP addressing



requirements, and/or managed service fees. The Service does not support non-integrated, third party HA solutions.

3.7.1.1.1.2 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. Under this option two sockets may be configured and deployed—one fully operational, and the other serving as a backup should the first appliance fail.

3.7.1.2 Zero Trust Network Access (ZTNA)

3.7.1.2.1.1 ZTNA is a service that utilizes a zero-trust policy, that provides network access through continuous authentication and monitoring of Customer provided endpoints, applications and users to ensure compliance with Customer defined security parameters.

3.7.1.2.1.2

Service does not include IT troubleshooting of end point devices or their software; end point devices include but are not limited to computers and the software installed on them that is not directly related to the Service.

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 applicable service guarantees ("Service Guarantees") in Blackfoot Communications' Service Level Agreement posted on Blackfoot Communications' website (the "SLA"), which SLA is incorporated herein by this reference, are dependent upon Customer's compliance with Customer's contractual obligations and the following:

4.1.1 Operating Environment. Customer shall provide Blackfoot Communications with secure space sufficient to access and install socket(s) and circuits. Prior to installation Customer shall notify Blackfoot Communications if secure space has available space in an equipment cabinet or if the socket will require wall mounting.

4.1.2 Power. Customer shall provide power, including universal power supply (UPS).

4.1.3 Access. Customer shall provide Blackfoot Communications or Blackfoot Communications' third-party contractor access to the buildings and point(s) of demarcation at each Customer service location to allow Blackfoot Communications and its approved contractors to install the Service. Access will be granted during normal business hours (8am-5pm) and, if required, at any time, to resolve emergency service or to maintain the Service.

4.1.4 Point of Contact. Customer shall provide Blackfoot Communications with the name and contact information of the point of contact (POC) for installation, service activation, notices for Service interruptions, and any maintenance activities.



4.1.5 Connectivity. Customer will provide access to Customer-premises and relevant appliance(s) necessary for Blackfoot Communications to manage and monitor the Service. Additionally, Customer shall communicate to Blackfoot Communications any network or system changes that could impact the Service via the process in §3.6.3 above. Service activation may require device downtime.

5. ADDITIONAL RULES, REGULATIONS, TERMS AND CONDITIONS

5.1 Configuration. Blackfoot Communications has certified network engineers who follow industry standards regarding configuration.

5.2 Secure Access. Blackfoot Communications technicians remotely access Customer's managed devices through a secure (encrypted) and restricted connection. Blackfoot Communications shall have, and Customer hereby grants Blackfoot Communications, root access to Customer's sockets(s) managed hereunder during the Term.

5.3 Vendor Support Agreements. By signing below Customer authorizes Blackfoot Communications to purchase, on behalf of Customer, 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. Customer also understands that it may be indirectly bound to the terms and conditions associated with the Vendor services. Such terms can be found on the Vendor's website: <https://www.catonetworks.com/msa/>.

5.4 Transferrable Management. When Customer's contract with Blackfoot Communications relating to this Service expires or is terminated, Blackfoot Communications will remove (1) Blackfoot Communications' credentials for access to the Customer-owned device(s) and (2) Blackfoot Communications' proprietary 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.

5.5 Socket Replacements and Upgrades. The Service includes configuration time applied by Blackfoot Communications to upgrades and replacement Customer sockets of the same Vendor family.

5.6 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 updates—e.g. changes by Customer's compliance requirements (e.g., PCI, SOX, etc.) and/or other Customer-initiated audits or network changes.

5.7 Breach. In the event of a breach, Customer is solely responsible for incident response decisions, endpoint security, regulatory compliance, and Authorized User access. Customer is also solely responsible for device maintenance, updates and configuration decisions. Customer has not delegated, and Blackfoot Communications has not accepted, responsibility for breach prevention or regulatory determinations. 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. Since the Customer is solely responsible for all decisions relating to the security of their network, except where otherwise stated herein, the Customer agrees to defend and indemnify Blackfoot Communications harmless in the event of a breach. Should Blackfoot Communications determine that there has been unauthorized access to the Service (a breach), Blackfoot Communications will notify Customer and Customer will determine a course of action regarding the breach. If there is a determination, or reasonable belief that a breach has occurred, Customer hereby authorizes Blackfoot Communications to 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 Customer in its 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, Such cooperation will be limited to six months from the date of the breach and shall exclude expert testimony unless separately agreed. Customer will be billed at Blackfoot Communications' standard labor rates.

5.8 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, the 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, which the Parties agree Blackfoot Communications bears no responsibility for. At Customer's option, Blackfoot Communications may quote, procure and rebill to Customer, on the monthly Blackfoot Communications billing statement, such third-party circuits.

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

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

5.11 Reservation of Rights. Blackfoot Communications reserves the right to modify these Managed SASE Terms, including the SLA, without Customer's prior approval, in which case Blackfoot Communications will post the updated version of the Managed SASE Terms to Blackfoot Communications' website.

5.12 Order of Priority. To the extent the terms and/or conditions of Customer's Service Order or the documents/agreements referenced therein conflict with these Managed SASE Terms, the order of priority to determine which terms control shall be as follows: the Additional Terms and



Conditions box on the Service Order, then these Managed SASE Terms, then the Master Service Agreement