MANAGED ROUTER AND MANAGED MONITORING SERVICES TERMS AND CONDITIONS

Blackfoot Communications' Managed Router and Managed Monitoring Services ("**Services**") is provided to the customer ("Customer") by Blackfoot Communications, Inc., DBA Blackfoot Communications ("Blackfoot Communications"; "Blackfoot"), collectively referred to as the "Parties," for the **Services** incorporated under these Terms and Conditions ("Terms").

***IMPORTANT ***

MANAGED ROUTER/MANAGED MONITORING IS FOR BUSINESS CUSTOMERS ONLY AND WILL BE MANAGED BY BLACKFOOT COMMUNICATIONS ON BEHALF OF CUSTOMER

In relation to the **Services**, the Parties agree:

1. Blackfoot Managed Router and Managed Monitoring Services includes:

1.1 Basic and Advanced Router Management; and

1.2 IntuiNet Network Dashboard, which includes:

1.2.1 Blackfoot's advantageous use of the SolarWinds application, a network monitoring and management software package, and provides Customer with a dashboard, a read-only view of the Blackfoot Communications' portion of Customer's network. Using IntuiNet, Customer may monitor circuit activity and receive selected types of alerts as described further herein.

1.2.2 Features and Functionality

1.2.2.1 Basic IntuiNet provides customers with the following:

1.2.2.1.1 The ability to monitor a wide array of network statistics such as bandwidth utilization, errors and events. Typically, devices are polled every two minutes (polling: refers to actively sampling the status of a device by a client program, in this case, SolarWinds); and

1.2.2.1.2 The same status information (view) that Blackfoot's Technical Assistance Center (TAC) receives concerning status changes on Customer's network.

1.2.2.2 Advanced IntuiNet with provides customers with alerts, based on Customer's requirements, and automatically sends an email or text message (or both) to Customer in the event of an outage to publicly accessible device or web site. Types or alerting covered are:

1.2.2.2.1 Up/down status of both on net and off net monitored devices (must be publicly addressed and have ICMP allowed from Blackfoot Communications' polling servers).

1.2.2.2.2 Up/down status of specific websites (must be publicly-addressed and have ICMP allowed from Blackfoot Communications' polling servers)

2. Managed Routers - Business Conditions

2.1 Managed Router Services cannot be sold as a standalone service to customers and must be sold with other Blackfoot Communications services, such as circuit services (e.g., Ethernet, Internet, Multiprotocol Label Switching (MPLS)).

2.2 When Customer purchases both Blackfoot circuit services and Managed Router Services and then when Customer does not renew the data circuit contract, Blackfoot Communications may end the Managed Router services with Customer.

3. Basic and Advanced Managed Router and Managed Monitoring Services include:

3.1 24/7/365 Network Operations Center Monitoring

3.1.1 Blackfoot Communications monitors Customer's routers with 24/7/365 network monitoring of device up/down. Blackfoot Communications technicians will be alerted of connections going down and certain connectivity problems.

3.1.2 Blackfoot's monitoring captures a range information on bandwidth utilization, and typically, a range of additional items on each device is setup for monitoring. Monitored items include, but are not limited to, response time, packet loss, hardware health and other critical items.

3.1.3 Alerts to Blackfoot Communications' Technical Assistance Center (TAC) is set on the circuit up/down status.

3.2 Troubleshooting and Resolution. Services includes troubleshooting and resolution during Blackfoot Communications' normal business hours. Services provides a 24-hour turn-around for customer requested configuration changes during normal business hours.

3.3 After Hours Support. After-hours support is available to Customer at current after-hours support rates with a 2-hour minimum (Two hours minimum is required for on-call technician to establish a secure computer log in, review network monitoring info, make an assessment, contact Customer, and complete resolution in consultation with Customer.)

3.4 Best Practice Expert Configuration. Blackfoot Communications has Cisco and Juniper certified engineers capable of complex configurations based upon industry standards.

3.5 Secure Access (encrypted). Blackfoot technicians shall only remotely access Customer's managed devices through a secured, restricted (encrypted) SSH connection.

3.6 Software Updates. Blackfoot Communications follows industry best practices and therefore, not all vendor software updates are routinely applied. Router updates will be applied as needed and in consultation with Customer.

3.7 Off-net Router Management. Services provides support of edge routers connected to third party circuits (off net). Blackfoot Communications provides the same level of service as with on-net router management, however, services may be limited by variables introduced by use of a third party network which are beyond Blackfoot Communications' ability to troubleshoot and control. Functions such as QoS will be limited due the nature of third party (off-net) circuits.

3.8 Configuration Archiving. Blackfoot Communications archives the most recent configuration of Customer's router for backup and restore purposes.

3.9 Support Agreements. Customer is strongly encouraged to have an active SmartNet or similar vendor support contract. If a support agreement is not in place, Blackfoot Communications may be unable to apply vendor updates, fix issues, or assist in coordinating a Return Merchandise Authorization (RMA).

3.10 Transferrable Management. When Customer's contract terminates, Blackfoot Communications will leave the router configuration on Customer's device intact, however Blackfoot will remove its credentials for access to that device and its proprietary router configuration (e.g., Blackfoot's proprietary configuration would mainly include things like passwords and logging to external servers, but may also include any configuration that we've developed in-house that other providers do not offer.) This service does not include assistance in migrating to other providers.

3.11 Router Replacements and Upgrades. Services excludes configuration time applied by Blackfoot Communications to new customer routers (e.g. new/upgraded routers, replacement units that need configuration). Configuration is billed to Customer at current Blackfoot rates and with prior consultation.

3.12 Support for most servers and network devices. PING, HTTP, HTTPS, DNS, FTP, POP3, SMTP's IMAP, SSH, Telnet, My SQL, MS SQL, and Custom servers and devices. Custom port monitoring allows testing the connection to any TCP/UDP service.

3.13 Other Terms and Conditions.

3.13.1 Changes constituting a customer initiated redesign may be subject to Blackfoot Communications' current hourly rates.

3.13.2 Other project work is not included including significant router updates due to customer PCI or other customer-initiated audits.

4. Advanced Router Management. In addition to the services described in Basic Router Management, Advance router management additionally includes:

4.1 Quality of Service Configuration. Best-practice, standards-based prioritization of network traffic based upon customer LAN requirements. Examples would be prioritizing voice over data traffic, or a specific application such as Citrix (e.g., terminal services). Limited QoS support is provided to edge routers on Internet circuits (e.g., Blackfoot Communications can configure a policy but it is not guaranteed on Internet circuits).

4.2 Advanced VPN Configuration (IPSEC, GRE, DMVPN). Best-practice, standards-based configuration of multi-site WAN connectivity based upon customer requirements.

4.3 Router Firewall Management. Management of software-based firewalls on Cisco and other supported routers. This service does not include management of hardware firewalls.

4.4 Failover Management. Failover between Blackfoot Communications provided circuits is provided (off-net circuits are excluded).

5. Related Router Management Services Available for an Additional Fee (see descriptions above)

5.1 **Remote Client VPN configuration.** Example: Home users doing remote access to the office.

5.2 **Third Party VPN configuration.** Example: Blackfoot Communications manages Customer's router, but customer subscribes to third party service and therefore we are only able to manage one end of the VPN connection.

5.3 **Customer / Third party device management**. Example: Customers that have a device like a SPAM filter, content filters, any network device, and that need our assistance in configuration setup, changes, etc.

6. Additional Notes

6.1 Only includes devices that Blackfoot Communications would add for its own internal monitoring of a customer's Blackfoot Communications circuit (i.e., Customer cannot request that Blackfoot Communications add their Charter circuit at another location to IntuiNet monitoring).

6.2 Additional Blackfoot Communications IT support to Customer is usually available for an additional time and materials charge at the-then current Blackfoot Communications rates.