Blackfoot Hosted Server Terms & Conditions

1. Introduction

Blackfoot Hosted Server is a family of cloud-based business services that enables employee collaboration via file and application sharing, individualized workspaces and shared areas, delivery of virtual desktops and disaster recovery capabilities. Blackfoot provides three tiers of services:

1. Basic Server **- Tier 1**
2. Office Server **- Tier 2**
3. Office Server Pro **- Tier 3**

Standard Service Model Options

Blackfoot provides customers with services on a 12, 24, 36 or 60-month subscription term. Services are available in three choice-of-service models in the below base configurations:

- **Tier 1:** Provides 2vCPU, 2GB vRAM, 50GB HD, and a 50Mbps/50Mbps Internet connection with Windows Server. This is an unmanaged service providing customers with administrator access to their virtual server
- **Tier 2:** Provides 2vCPU, 4GB vRAM, 200GB HD and a 50Mbps/50Mbps Internet connection with Windows Essentials/Standard. This is a managed server providing customers with "super user" access while Blackfoot retains root access.
- **Tier 3:** Provides Tier 1 + Tier 2 in a combined solution with a 50Mbps/50Mbps Internet connection while Blackfoot retains root access.

In consultation with Blackfoot technical support, customers may upgrade CPU, RAM, storage, and bandwidth resources at then current pricing. Additional options such as SQL licensing, Microsoft O365 services, or Microsoft Office client licensing are available at then current pricing.

All Services include:

- Base configuration shown above with optional add-ons (at then current pricing)
- HP servers and Intel XEON processors
- Virtuozzo virtual machine (VM) infrastructure
- All virtual machine and Microsoft operation system (OS) licensing (Windows Server 2012; Windows Essentials R2 2012)
- Virtual machine infrastructure support, monitoring, and security as described herein.
- Single Static IP Address

- Cisco ASAV firewall and VPN
- Free applications upon customer request (Adobe Reader, JAVA, Firefox, Chrome, Silverlight)

Managed Services include:

- Basic server migration (included services are detailed below)
- Vipre Anti-Virus application and management
- Domain controller and active directory management

2. Service Operations

The following outlines Blackfoot's roles and responsibilities in the delivery of services. While specific roles and responsibilities have also been identified as being owned by the customer ("Customer"), any roles or responsibilities not contained in this document are either not provided with the service or assumed to be Customer's responsibility.

2.1 Services – General

Blackfoot will use good faith efforts to implement the Services as set out in the Service Order. It may be necessary for Customer to assist Blackfoot in this implementation before and during the Term (defined below) of this Agreement. Customer agrees to provide reasonable cooperation and assistance, and to cause any of Customer's third-party providers to do so as Blackfoot.

If Blackfoot provides or resells certain software or services to the Customer, Customer understands and agrees that they may be bound by additional terms and conditions imposed by applicable third-party vendors or licensors.

2.2 Blackfoot Obligations

In addition to providing the Services to Customer as set out in this Support Policy, our Service Level Agreement (SLA) sets out Blackfoot's commitments to Customer, and all terms and conditions are governed by Customer's Master Services Agreement (MSA) with Blackfoot.

Blackfoot agrees to provide the Services set forth on the Service Order. However, from time-to-time Blackfoot may modify the Services should a vendor no longer provide components of them to Blackfoot, the technology change, or to account for our operational needs. Blackfoot will use reasonable efforts to secure substitute services for the remainder of Customer's MSA term. Should Blackfoot be unable to secure those services in a reasonable manner Blackfoot may terminate the Services, or that aspect of the Services so affected.

2.3 Customer Obligations

Blackfoot relies on the information Customer provides to Blackfoot and in the Service Order for services. Customer agrees (a) to keep their information up-to-date, and (b) that Blackfoot may rely on the accuracy of this information.

This Agreement grants Customer a license to use the Services, and any third-party components incorporated into them. Title remains with Blackfoot, or Blackfoot's licensors. Customer may not reverse engineer, decompile, or otherwise attempt to derive the code underlying these items

3. Service Provisioning

Blackfoot will provide the following initial provisioning of services:

Managed or Unmanaged Services:

- Implementation of service components (hosted servers and network devices) needed to support Customer contracted services.
- Initial resources for hosted services (IP address, memory, processing, storage, and networking).
- Enabling a secure point-to-point network interconnect via a VPN from Blackfoot to Customer's remote location.

Managed Services:

- Basic Server Migration includes migrating Customer's existing server data and Microsoft applications to the Blackfoot Hosted Server.
- Providing initial training on accessing hosted server(s), implementing user accounts, establishing Blackfoot provided VPN connectivity to Customer's authorized account representatives (if Customer opts to use their P2P VPN, Blackfoot will provide IP address for Customer use).
- Providing access to self-service training materials [e.g., reference user documents].
- Provisioning services provided during normal Blackfoot business hours (after hours provisioning, data migration, custom migrations are at then current after hours rates).

Unmanaged: Services

- Instructions on server access and login.

Customer will be responsible for the following provisioning services:

- Assisting Blackfoot with migration of Customer data and unique or industry specific applications.
- Providing timely access to existing server and employee workstations or user profiles needed to facilitate Blackfoot's migration of data and applications.

4. Disaster Avoidance and Disaster Recovery

Blackfoot will provide the following services with respect to Disaster Avoidance and Disaster Recovery:

Unmanaged Servers	Managed Servers
Enable Customer to create server backups via PowerPanel and Customer will do own restore of backup file.	No Backups
Server snapshots (optional add-on), Blackfoot does restore	Server snapshots – 5 calendars days are stored; Blackfoot does restore
File Backups (optional Blackfoot RDB as add-on or third party solution). Blackfoot installs RDB, Customer manages. Customer installs and manages any third party solution.	File Backups. Optional Blackfoot Remote Data Backup (RDB) or third party solution. Blackfoot installs RDB or third party solution. Customer manages Blackfoot or third party solution.

5. Service Requests and Server Configuration Changes

A. Service requests

Normal Business hours:

Toll Free Phone: 1-877-881-1155

Email: NOC@blackfoot.com

After Hours/Weekends/Holidays

Toll Free Phone: 1-877-881-1155

B. Service request response time

Blackfoot will take all reasonable actions to respond to service requests within two (2) hours at any time of the day. After hours incurs after hours T&M charges, 2 hour minimum.

C. Server Configuration Changes

Customers that wish to upgrade or downgrade their server configuration should contact their assigned Blackfoot Sales Account Executive. If your Account Executive is not known, please call us at the number above.

Changes to server CPU and RAM resources require a virtual machine (server) restart resulting in (typically) a brief service interruption. A storage space increase does not require a restart.

6. Server Monitoring

Blackfoot will provide monitoring and notification to Customer's authorized representatives for the services listed below:

Unmanaged Servers	Managed Servers
VM infrastructure	VM infrastructure
VPN accessibility	Customer server (VM)
	Resource utilization (vCPU, RAM, storage)
	Vipre anti-virus
	VPN accessibility

7. Incident and Problem Management

Blackfoot will provide incident and problem management services (e.g., detection, escalation, and return to service) pertaining to:

- Infrastructure over which Blackfoot has direct, administrative, and/or physical access and control, such as physical servers, storage and network devices.
- VPN accessibility.
- Blackfoot provided / licensed software: Examples include Microsoft 0365, SQL server, Office Blackfoot will open a ticket, at Customer's request and with Customer assistance, with the licensing entity, and Blackfoot and Customer will monitor the issue resolution.
- Operating system administration including the operating system itself or features or components contained within the provided operating system (Managed Servers only).
- Anti-virus system management (for managed server services) Note: Virus removal is subject to additional fees.

Customer is responsible for incident and problem management (e.g., detection, escalation, and return to service) pertaining to:

- **Unmanaged Servers**: Customer is responsible for the server and all it contains (unless noted otherwise herein).
- **Managed Servers**: Customer is responsible for notifying Blackfoot of any performance concerns with provided server or Blackfoot provided applications (e.g., licensed software)
- **3rd Party or Proprietary Software:** Customer provided 3rd party or proprietary applications (incident management with Customer's provider).
- Performance of Customer databases.
- Operating systems customized by Customer, or other assets deployed and administered by Customer that are unrelated to the services provided.
- Anything else not under the direct control and administration of Blackfoot operations.

Server Change Management

Managed server included services:

- Resource monitoring and notifications
- Updates and patches to the Microsoft OS, Vipre anti-virus, and site-to-site VPN
- User account management
- Snapshot restoration
- Assistance with file restoration

Managed server excluded services:

- Customer specific / industry specific software installation, patching, removal or support.
- Excessive amount of user account changes in a month
- Excessive file restorations

- Support of third party and Customer provided software applications loaded onto servers in conjunction with Blackfoot provided OS versions.

8. Security

The end-to-end security of the service is shared between Blackfoot and Customer. Blackfoot will provide security for the aspects of the service over which it has sole physical, logical, and administrative level control.

Customer is responsible for the aspects of the Service over which Customer has either administrative or root level access or control. The primary areas of responsibility shared by Blackfoot and Customer are outlined below.

Blackfoot will use industry standard methods and best practices to secure the Services. Many of the resources associated with the services are co-managed with Customer. Customer agrees to provide Blackfoot with information that will allow Blackfoot to configure the services in a way that meets Customer's security needs. Should Blackfoot determine that there has been unauthorized access to the server (a breach), Blackfoot will notify Customer as soon possible and Blackfoot and Customer will work together to determine a course of action with regard to the breach. Blackfoot may take action, including suspending all, or part of the Services, to isolate and mitigate the cause of a Breach. The breach notification may contain preliminary and unconfirmed information; however, it is provided to Customer to assist in efforts to mitigate the effects of a breach. Blackfoot and Customer each agree to reasonably cooperate with each other to investigate the facts and circumstances involved in a breach. To the extent Blackfoot's cooperation requires time and resources above and beyond those extended by us in conjunction with a typical breach investigation, or should Blackfoot be asked to cooperate with a governmental investigation, Customer will be billed at Blackfoot's standard labor rates.

Blackfoot will use commercially-reasonable efforts to provide:

- **Physical Security:** Blackfoot will protect its data centers housing the service from physical security breaches using security best practices.
- **Information Security:** Blackfoot will protect the virtual machine infrastructure used to deliver the service for which it has sole administrative level control.
- **Network Security:** Blackfoot will protect the networks containing virtual machine infrastructure.
- **Security Monitoring:** Blackfoot will monitor for security events involving the underlying infrastructure servers, storage, and networks used in the delivery for which it has sole administrative level control.
- **Patching & Vulnerability Management:** Blackfoot will maintain the systems it uses to deliver the service offering, including the application of patches it deems critical for the systems.

Customer should address:

- **Information Security:** Customer is responsible for ensuring adequate protection of the information systems, data, content or applications that Customer installs or accesses. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to Customer internal, external, or third party users, etc.
- **Network Security:** Customer is responsible for the security of the networks over which Customer has administrative level control.
- **Security Monitoring:** Customer is responsible for the detection, classification, and remediation of all security events that are isolated with Customer account, associated with server, operating systems, applications, data, or content, surfaced through vulnerability scanning tools, or required for a compliance or certification program in which Customer are required to participate and which are not serviced under another Blackfoot security program.
- **Compromised Devices**: Customer is responsible for any compromised desktops, laptops, or other devices accessing the services and resolving related issues. Blackfoot reserves the right to suspend desktops or whole Customer accounts if compromised desktops are detected in order to protect Blackfoot's infrastructure and business operations.

9. Compatibility Table

Blackfoot uses supported Microsoft operating system, server, and Office applications. Currently supported software is listed at the Microsoft site:

Microsoft Lifecycle Support: https://support.microsoft.com/en-us/lifecycle/search

Service and support issues may arise if Customer is using applications that are no longer supported by Microsoft.