Schedule 3 emPOWER Cloud Services (IaaS)

1   Service Description

1.1   The emPOWER Cloud Services comprise a pillar of the emPOWER Managed Services portfolio and are made up of discrete service offerings and products as set out below.

1.2   The emPOWER Cloud Services are designed to provide you with high performance infrastructure environment that is owned, hosted and managed by us, that you can access and use to run your applications during the Managed Service Period. Our infrastructure environment connects with your Customer Network Equipment at your router. The details of the specific emPOWER Cloud Services, the Minimum Managed Service Requirements, Managed Service Period, Minimum Spend, Fees and other details will be set out on the Service Order.

1.3   The emPOWER Cloud Services are specified in terms of the capacity and performance of the emPOWER Cloud Services being provisioned and not a description of the hardware used to provision those emPOWER Cloud Services. These metrics will be specified on the Service Order.

1.4   We will supply to you with the emPOWER Cloud Services specified in the Service Order, initially in the quantities specified in the Service Order and otherwise as specified in writing by you from time to time at the Fees specified in the Service Order.

1.5   We regularly upgrade and update the technology we use to provide the Managed Services (e.g. a more efficient version of the software controlling the virtual server hosts becomes available, or that software has better features, or that software may become end of life and need to be upgraded to maintain critical vendor support). This means that the emPOWER Cloud Services are continually evolving. Some of these changes will occur automatically, while others may require us to schedule and implement the changes. The changes may also mean that you need to upgrade your Customer Network Equipment in order to make efficient use of the emPOWER Cloud Services. We will provide you with advance notification in this case.

1.6   We recognise that you may have legitimate business reasons for not upgrading to a new version of the emPOWER Cloud Services as soon as the version becomes available. However, we will not support old versions indefinitely. When an old version used by you is at end-of-life, we may upgrade you to a new version.

Compute Service

1.7   This component of the emPOWER Cloud Service provides you with dedicated and virtualised infrastructure resources that are located in our managed Data Centres and delivered as a service.

1.8   You may apply for one or more of the following compute offerings:

(a)   Virtual server;

(b)   Self-managed virtual server;

(c)   blueAPACHE managed virtual server;

(d)   blueAPACHE managed physical server.

1.9   We do not provide you with physical access to the server infrastructure.

Operating Systems Service

1.10   This component of the emPOWER Cloud Service provides you with a choice of pre-packaged operating systems for use with your virtual or physical server(s).

1.11   If you have an existing License to use one of the pre-packaged operating systems which are set out in the Service Order, you may use your existing operating system License provided that you comply with the third party supplier's software licensing terms and your operating system meets any compatibility requirements specified by us from time to time.

1.12   Where you provide your own operating system License you are responsible for obtaining and maintaining an appropriate License to use the operating system you provide on the blueAPACHE Environment.

Storage Service

1.13   This component of the emPOWER Cloud Service provides you with access to storage capacity that can be used by you for various purposes including to store your Customer Data and applications.

1.14   The Storage Service includes:

(a)   a data repository which may be partitioned into virtual disks for storing application, operating system and file system data (you may request that we create additional disk partitions and we may charge you a Fee); and

(b)   levels of hardware redundancy.

1.15   As part of the process for provisioning your Storage Service, you may have existing Customer Data which you wish to migrate. Should you require assistance in the migration of your Customer Data, we will consult with you and provide advice and technical assistance on the migration of your Customer Data for an additional Fee.

1.16   Once a disk has been created in your storage repository the storage capacity of the virtual disk cannot be decreased.

1.17   If you wish to decrease the storage capacity of a disk, you will need to create another disk that meets your revised storage capacity requirements and then transfer the contents of the original disk to the new disk.

1.18   You are responsible for ensuring that all disks provided under the Storage Service have sufficient free storage capacity in accordance with the system requirements for the relevant operating system you have selected.

Backup Service

1.19   This component of the emPOWER Cloud Service provides you with a facility to backup and restore different components of your Customer Data on servers located in our managed Data Centres in the event of data corruption.

1.20   The Backup Service backs up your operating system data and file data that is not otherwise being accessed at the time of the backup, in accordance with your Service Order.

1.21   The type and amount of Customer Data that will be backed up and the duration and frequency at which it is kept during the Managed Service Period will depend on configuration set out on the Service Order.

1.22   We will retain daily copies of Customer Data within the data repositories accessed by the servers and configured for backup for the retention periods set out in your Service Order.

1.23   We will retain your backups of Customer Data that your Service Order states is subject to the Backup Service only during the Managed Service Period. You must ensure that you have extracted copies of all Customer Data that you require from the Backup Service prior to the end of the relevant Managed Service Period.

1.24   We may not be able to provide you with the Backup Service if you make certain changes to your Customer Network Equipment or Customer Software. For this reason, you must tell us when you make changes that could affect the Backup Service so that we can let you know whether your Backup Service is likely to be compromised. We cannot guarantee that backups created by the Backup Service will be uncorrupted or error-free or capable of being restored.

1.25   Our Backup Service will create backup copies of the application data only where you have requested us to install the software plug-in for the specific application you wish to be backed up. If you do not request the installation of the appropriate software plug-in, the Backup service will create a data file backup of your application; however your Backup service will not create an application level backup of your application data.

1.26   If you require the Backup service to backup your structured application or database data, you are responsible for backing up such data in accordance with any instructions provide.

1.27   In the event that a backup restoration is required, we will provide you with the backup files that you specify. You are responsible for the recovery of individual files from those backup files.

1.28   Our Backup service is designed for data sources where the average daily change rate in a week of backups per server is five percent or lower. If your average daily change rate in a week is greater than five percent you may have to pay an additional Fee (which we will notify you of) or we may cancel your Backup Service.

Anti-Virus Service

1.29 This component of the emPOWER Cloud Managed Service provides you with a software based anti-virus capability. We use industry leading Anti-Virus software configured to the manufacturers' installation guidelines and manage in accordance with the manufacturers' instructions.

Intrusion Prevention Service

1.30 This component of the emPOWER Cloud Service provides you with an end-point software based intrusion detection capability.

1.31 You must provide us with 7 Business Days' notice before you undertake vulnerability or penetration testing of your network.

1.32 This service is not available on the virtual server and self-managed virtual server based Managed Services.

Virtual Server Service

1.33 This component of the emPOWER Cloud Service provides you with a choice of virtual server configurations to run on our virtualised and multi-tenanted infrastructure platform. Your selection for the various configuration options will be set out on the Service Order.

1.34 We do not provide a facility for you to use accessories or peripheral devices with your server infrastructure (such as USB attachments or License key dongles).

1.35 Prior to our execution of some service requests (including changes to your CPU and RAM configurations and restoration of storage snapshots) we may request that you power down the relevant virtual server(s). We may be unable to address your service request until you have disabled the relevant virtual server(s).

1.36 You must nominate a system administrator to manage your servers and user access to the management console. You may request that we activate additional users or change existing user access privileges to the console.

1.37 If your service includes a VPN service, you will be responsible for loading and configuring any VPN software on your Customer Network Equipment.

1.38 Our virtual server service does not support customer supplied operating systems for use with the operating system under the virtual server offering and you must select one of our pre-packaged operating systems, the details of which will be set out on the Service Order.

1.39 If you are not receiving the emPOWER Managed Services (under Schedule B), you are responsible for configuring and monitoring your operating system and ensuring that your operating system is up to date by installing updates when the operating system software notifies you that an update is available.

1.40 If you have acquired the Storage Service in combination with the Virtual Server Service the Storage Service includes a facility which enables you to create a single snapshot copy of your Customer Data which is stored within our managed Data Centre for 24 hours, including your virtual server configuration data and data stored in RAM and on your virtual disks. We retain snapshots within our managed Data Centre for 24 hours unless overwritten by another snapshot or deleted by you.

1.41 The snapshot facility is provided for the purposes of reinstating a point in time snapshot of your server's configuration and data in the event of a service failure and we do not provide the snapshot to you for backup or archival purposes.

Managed Physical Server Service

1.42 This component of the emPOWER Cloud Service provides you with a dedicated blueAPACHE Environment which is reserved for your use.

1.43 You may select from various base dedicated infrastructure options, which will be set out on the Service Order.

1.44 With this emPOWER Cloud Service we do not provide a facility for you to use accessories or peripheral devices with your infrastructure (such as USB attachments or License key dongles).

1.45 Some of your service requests (including changes to your CPU and RAM configurations and restoration of backup snapshots) under this emPOWER Cloud Service may require you to power down the relevant virtual or physical server(s). We may be unable to address your service request until you have disabled the relevant virtual or physical server(s).

1.46   Your Managed Physical Server Service includes:

       (a)   monitoring and management of the dedicated blueAPACHE Environment allocated to you;

       (b)   patch management with respect to the operating system and Anti-Virus software

1.47   You need to nominate a system administrator to manage your customer portal account. You may request that we activate additional user accounts or change existing user accounts and access privileges for use with the online portal for an additional Fee.

1.48   If your service includes a VPN service, you will be responsible for loading and configuring any VPN software on your Customer Network Equipment.

On-Premise Private Cloud

1.49   This component of the emPOWER Cloud Service provides you with a managed virtual server on your infrastructure and may include us providing you with third party software under additional License terms to be agreed with us and/or the third party licensor.

1.50   You may request that we create or reduce virtual servers on your behalf, subject to an additional Fee.

1.51   You may request that we create or reduce the capacity of a virtual disk on your behalf, subject to an additional Fee.

1.52   Your allocation of CPU and RAM resources to virtual servers may not exceed the total resource capacity purchased by you for your server infrastructure in accordance with your Service Order.

1.53   You must notify us before you cause one of your virtual servers to restart or reboot or make any changes to the configuration of any applications running on your servers.

On Premise Customer Managed Virtual Data Centre Service

1.54   This component of the emPOWER Cloud Service provides you with a self-managed virtual Data Centre environment on our infrastructure.

1.55   You will have access to a management toolset that provides limited access for the purposes of creating and managing your virtual servers.

1.56   You may use the management toolset to create and configure virtual servers to which you may allocate CPU and RAM resources.

1.57   You may use the management toolset to create and configure virtual disks.

1.58   Your allocation of CPU and RAM resources to virtual servers may not exceed the total resource capacity purchased by you for your server infrastructure in accordance with your Service Order.

1.59   In the event of an impact to your Self-Managed Virtual Data Centre Service through your use of the management toolset, we will attempt to help you reinstate your service or recover your Customer Data but we do not guarantee that we will be able to fully restore your service or any Customer Data.

1.60   You are responsible for sourcing, installing and configuring all end-point security software which you wish to install on your virtual servers (including anti-virus and intrusion prevention software).

1.61   The management toolset is a sophisticated tool and you are responsible for obtaining adequate training and certification in the use of the hypervisor management toolset we provide you with access to.

Backup & Recovery for Customer Equipment at Customer's Premises

1.62   This component of the emPOWER Cloud Service provides you with a facility to backup and restore your Customer Data from your hardware/operating/network system located on your Premises in the event of data corruption or failure.

1.63   The type and amount of data that will be backed up and the duration for which it is retained will depend on your chosen configuration, and will be set out in the Service Order.

1.64   We will retain daily copies of Customer Data within the data repositories accessed by the servers and configured for backup for the retention periods set out in your Service Order.

1.65   We will not retain your backups after the end of the Managed Service Period.

1.66   Backup of servers on your premises:

    (a)   can only be provisioned over a private network provided by us; and

    (b)   is subject to you installing a software agent on your servers and agreeing to License terms to be agreed with us and/or the third party licensor.

1.67   This Backup Service backs up your Customer Data that is not otherwise being accessed at the time of the backup, in accordance with your Service Agreement.

1.68   We may not be able to provide you with the Backup Service if you make certain changes to your hardware/operating system/network or Customer Software. For this reason, you must tell us when you make changes that could affect the Backup Service so that we can let you know whether your service is likely to be compromised. As our Backup Service takes a copy of your Customer Data, which may or may not be error free at the time of backup, we cannot guarantee that backups created by the Backup Service will be uncorrupted or error free

1.69   Our Backup Service will create backup copies of the application data only where you have installed the software plug-in for the application you wish to be backed up. If you do not install the appropriate software plug-in, the Backup Service will create a data file backup of your application; however your Backup Service will not create an application level backup of your application data.

1.70   Our Backup Service will create backup copies of the application data which you have exported to a virtual disk. If you do not export the application data to a virtual disk, the Backup Service will create a point in time backup of your application (which will include your application data); however your Backup Service will not create a data file backup of your application data.

1.71   If you require the Backup Service to backup your structured application or database data, you are responsible for backing up such data in accordance with any instructions we provide you.

1.72   In the event that a backup restoration is required, we will provide you with the backup files that you specify. You are responsible for the recovery of individual files from those backup files.

1.73   Our Backup Service is designed for data sources where the average daily change rate in a week of backups per server is five percent or lower. If your average daily change rate in a week is greater than five percent you may have to pay an additional Fee (which we will notify you of) or we may cancel your Backup Service.

Security Service

1.74   This component of the emPOWER Cloud Service provides you with a secure hosted internet gateway located in our managed Data Centres.

1.75   You may apply for one or more of the following security offerings:

    (a)   Dedicated Gateway;

    (b)   Firewall;

    (c)   Internet Protection Services;

    (d)   Denial of Service Protection (DoSP);

    (e)   Intrusion Protection.

Data Import and Data Export Service

General

1.76   This component of the emPOWER Cloud Service enables you to transfer your Customer Data to and from your chosen Hosting or Backup products via a physical storage device ("Device").

1.77   The Data Import and Data Export services will usually be performed during Business Hours. An additional Fee may apply if you request Data Import or Data Export Services outside Business Hours.

1.78   You must comply with the instructions we provide to you in connection with the transfer of your Customer Data.

1.79   If we supply you with a Device and you have not returned the Device to us within one month of receipt, we may charge you for the replacement cost of the Device at our then current Fee.

Data Import

1.80   Upon request, we may provide you with a Device for you to transfer your Customer Data onto and return to us.

1.81   Following receipt of the Device, we will notify you once we have connected the Device to your chosen service and you can then transfer Customer Data to the appropriate server(s).

Data Export

1.82   You will provide us with a Device for us to transfer your Customer Data onto and return to you. The Device must be blank and sufficient to hold the quantity of data you require transferred. Alternatively, we can supply a Device, at our then current Fee.

1.83   Following receipt of the Device, we will connect the Device to your chosen service and we will then copy Customer Data from the appropriate server(s) to the Device.

1.84   Once we have copied the data from the server(s) to the Device, we will notify you that the Device is ready for collection. Alternatively, upon request, we will return the Device to you via our nominated courier.

1.85   We will retain Customer Data on your server(s) until the sooner of the end of the relevant Managed Service Period or you request that we delete the data. After this date we will securely delete Customer Data.

Liability

1.86   Unless you supply your own Device, we retain title to the Device at all times. Risk of loss or damage to the Device and any Customer Data stored on it is with you whilst in transit or is in your custody or control. You should insure the Device and Customer Data whilst in transit. If one of our Devices that we have provided to you is lost, stolen or damaged whilst it is in your custody or care of in transit between you and us, we will charge you for a replacement Device at our then current Fee.

1.87   You are responsible for protecting your Customer Data on the Device. We strongly recommend that you encrypt your Customer Data prior to loading it on the Device in accordance with best industry practice and in accordance with the instructions we provide with the Device.

1.88   We are not responsible for any loss, theft or damage to the Device or your Customer Data other than as a direct consequence of our negligence.

1.89   You are responsible for ensuring that you comply with all applicable laws and have all necessary rights to provide Customer Data to us for transfer onto your server(s). You acknowledge we may need to reproduce Customer Data to transfer it between the Device and your server(s).

Third-Party Licensing Compliance

1.90   blueAPACHE may, from time to time, be instructed by our third-party software providers to conduct software licensing compliance investigations. This will involve the execution of compliance applications/tools on your infrastructure. You will be notified when we intend to conduct the investigation, and your permission for us to do so may not be unreasonably withheld.

Other Customer responsibilities

1.91   You must ensure that, at your own cost:

(a)   you comply with any requirements on the Service Order;

(b)   all our equipment and your equipment is located at the sites in such manner and position as is reasonably requested by us to enable us to undertake the Managed Services;

(c)   You must have a high-speed Internet connection to access the emPOWER Cloud Services, and hardware and software that are compatible with the emPOWER Cloud Services.

1.92 You will be given a high degree of control over your operating system configuration and management. If you configure and manage your operating system in such a manner that causes disruption to the emPOWER Cloud Services and/or deletion of any data, you will be responsible for any loss that we suffer as a result and you may need to pay us an additional charge to fix any problems.

Service Requirements

1.93 We must provide the emPOWER Cloud Services in accordance with the requirements set out in the following table:

Planned Downtime	We must ensure that all Planned Downtime is undertaken outside Customer Operating Hours.
Data backup	Where you have purchased Backup Services we must ensure that all Customer Data is backed up nightly to servers located within a tier 2 or 3 Data Centre and separate to the servers specified in the Service Order;
Retention period for backed up Customer Data	We must ensure that all backed up Customer Data is retained for a minimum retention period of 30 days or until the end of the Managed Service Period, whichever is the sooner.

2   Exclusions from Scope

Management of the Cloud Systems

2.1 If you purchase an On-Premises self-managed virtual Data Centre (vDC) then management of VM's within the vDC are not our responsibility unless specifically set out on the Service Order.

2.2 We are not responsible for the monitoring, management or maintenance of your Virtual Machine operating system or applications unless you have procured emPOWER Managed Services from us under a separate Service Agreement (if so please refer to Schedule B – emPOWER Managed Services).

Other

2.3 Unless stated otherwise on the Service Order (and then only to the extent that it is set out on the Service Order) we are not responsible for:

(a)   backup of any Customer Data;

(b)   disaster recovery;

(c)   anti-virus or similar protection;

(d)   security.

3   Support Centre

3.1 We will provide you with access to our Service Centre during the Managed Service Period.

3.2 You must ensure that only your IT support team members who are skilled and knowledgeable in your technical and business environment and your applications make Incident Support Requests to Service Centre. In particular you must ensure that no end user contacts the Support Centre directly.

3.3 Your IT support team members may make Incident Support Requests to the Service Centre.

3.4 We will deal with each Incident Support Request made to the Support Centre as follows:

Incident Priority Definitions

Description	Definitions

All calls will be classified into one of the following severity levels:
- Priority One
- Priority Two
- Priority Three
- Priority Four
- Priority Five
	Priority One - Critical:
	Customer's ability to conduct business has stopped because of a failure of the Managed Service.
	    Examples: blueAPACHE Environment hosting one of more of Customer's Core Services is unavailable or unusable.
	
	Priority Two - Urgent:
	The Managed Service is seriously degraded but can continue its operation via a work-around or incremental resource for a short period of time before business stops.
	    Examples: Extremely slow system performance; network functionality becomes limited.
	
	Priority Three - Major:
	A failure in the Managed Service causes access to a Core Service or other managed application to be lost by a single or small number of users, affecting significant business functionality. Problems or incidents where a work-around exists or can be developed with a small amount of incremental resources.
	
	Priority Four - Ordinary:
	Problem or incident where single users can operate Core Services and other managed applications activities normal, but a definite fault is identified.
	
	Priority Five - Requests:
	Any call from single users or site groups that are requesting a new service or some clarification on an existing service.
	    Example: Requesting a new user logon, printer set up or the meaning of a system message.

Incident Resolution Control

3.5   Incident Support Requests are prioritised by us according to their impact and urgency. We aim to respond and resolve each case within the target timeframes in the following table:

Priority	Call Acknowledgement	Target Response	Target Resolution
Priority One	30 min	2 hours	4 hours
Priority Two	30 min	Same Business Day	1-2 Business Days
Priority Three	30 min	Same Business Day	2-3 Business Days
Priority Four	30 min	Next Business Day	3-4 Business Days
Priority Five (Service Request)	1 hour	Next Business Day	2–5 Business Days

Note: Each time period that is a minute or hour is calculated only during our Business Hours, unless you have acquired 24 x 7 Support from us, in which case these time periods are calculated on a 24 x 7 basis for Priority One incidents only.

3.6 In this table "Resolution" means an action that will resolve an incident, i.e., allows your users to carry out their business function even if this is achieved by using a temporary work-around, repair or alternative configuration, technology or process.

4 Service Levels

Service Level: System Availability

4.1 We provide Service Level in respect of the Availability of each System that is being managed under the emPOWER Cloud Service.

4.2 We must meet or exceed any Service Level that is applicable to each System that is the subject of the emPOWER Cloud Services acquired under the Service Order, except where the failure, delay or other breach arises from, or is contributed to by, a Reasonable Excuse.

Service Level Name	Service Level	Measurement
System Availability during Business Hours	99.9%	System Availability % is calculated as: 1-(Unplanned Downtime/Required Uptime) Where Unplanned Downtime and Required Uptime are measured over our Business Hours.
System Availability across the entire month	99.8%	System Availability % is calculated as: 1-(Unplanned Downtime/Required Uptime) Where Unplanned Downtime and Required Uptime are measured over the entire month.

4.3 In defining the Service Levels in this clause 4:

(a) **Planned Downtime** means the System is unavailable for a time period due to approved maintenance that is disruptive to system operation and usually cannot be avoided with a currently installed system design. Planned Downtime events might include patches to System software that require a reboot or System configuration changes that only take effect upon a reboot. Our policy is to agree a monthly downtime window with a Customer upon contract initiation during which planned downtime can occur at a time that causes minimal impact to Customer.

(b) **Required Uptime** means the total number of minutes in the month.

(c) **System** means the storage, compute and memory resources acquired by you as set out on a Service Order.

(d) **System Availability** means the % of time over the relevant period that the System is available to be used by either end users or other systems.

(e) **Unplanned Downtime** means any downtime that is not Planned Downtime during the relevant period.

How is the System Availability Service Level measured?

4.4 The Availability Service Level is measured and reported monthly. System Availability is measured by us using information obtained from our monitoring systems and is binding on us both.

5 Change Management

5.1 We will operate the following change management process:

Services	Description	Specifications
Change Management	The process to manage and track change requests to the Managed Services, systems and applications.	All change requests are to be submitted to the Service Centre. This functions as the control and tracking point for all changes. Change notification request periods are based on the type of change: Planned Projects - Two (2) weeks prior to change date. Non-Emergency – Five (5) days prior to change date. Emergency – Immediately as required#

- Should an **Emergency Change** be performed it must be as a result of imminent Emergency. All such changes will be retrospectively raised as a formal change and any associated major incident actioned and documented accordingly.

6 Service Period, Renewal and Termination

Service Period and Renewal

6.1 The commencement date of the Service Period of the emPOWER Cloud Services shall be the date when the Service under a Service Agreement commences which is:

(a) The earlier of the date that blueAPACHE notifies Customer that the Service is ready for use or the date that Customer first uses the Service, or

(b) such other date agreed by the Parties.

6.2 The Minimum Service Period of the emPOWER Cloud Services shall be 36 months, unless otherwise set out on the Service Order.

6.3 The Minimum Service Period (or any subsequent period of the Service Period) can be extended within the last 6 months of the Service Period for a subsequent Service Period of 36 months, or other such Service Period as agreed between the Parties, by requesting a revised Service Order quotation from blueAPACHE.

6.4 Should the Minimum Service Period elapse without Customer signing a revised Service Order, out of contract emPOWER Cloud Services list pricing will apply.

Termination for Convenience

6.5 You may terminate the emPOWER Cloud Services for convenience by giving us 30 days Written Notice. Early termination will attract an Early Termination Payment calculated using the following formulae:

Early Termination Payment = (A*B) + C,

where;

"A" is the Minimum Spend;

"B" is the remaining term of the Minimum Service Period; and

"C" is any outstanding Fees for work done or planned.

7 Pricing and Fees

Fees

7.1 You must pay the following Fees for the emPOWER Cloud Services in this Schedule:

(a) a variable monthly Fee, which can be renegotiated within 6 months of the current Service Period end date, with a view to extending as per Clause 6.3.

(b) the variable monthly Fee is based on the pricing schedule as specified in the Service Order;

(c) a Fee for Moves Adds and Changes ("MACs") as per the pricing schedule as specified in the Service Order.

Monthly Service Fee

7.2 Where there is a "Unit Price" (usually specified in the column headed "Quantity" in the Service Order), Fees must be calculated by reference to the quantity provided to you in the relevant month. The initial quantities required by you are usually set out in the column headed "Quantity" in the Service Order. You may change the quantities required for a month by giving written notice of the changes at least 5 days prior to the beginning of the relevant month.

Minimum Spend

7.3 Should the monthly Fee for any Managed Services fall below 50% of the initial charges for that Managed Service then a Minimum Spend equivalent to 50% of the initial Fees for that Managed Service shall apply.