Supplemental terms for the supply of MSP Services

TMB shall provide MSP IT support services to the Customer on the terms and conditions set out in TMB's General Terms and Conditions and the terms and conditions set out below. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in this Supplement.

1. SUPPLEMENTAL DEFINITIONS

1.1 'Alert' means an alert raised by TMB's Monitoring Agent in response to a detected Issue or potential Issue.

1.2 'Configuration' means the configuration of the Managed Equipment, including hardware, installed software and all associated settings and / or parameters.

1.3 'Data Centre' means TMB's UK- or EU-based remote data storage facility.

1.4 'End User' means a user of the Managed Equipment.

1.5 'Hardware' means IT equipment including Servers, Workstations, routers, switches and other electronic devices.

1.6 'Hours of Cover' means the hours of cover set out in the Service Schedule, unless amended on the Order.

1.7 'Lights Out Management' ('LOM') means Server-based functionality that enables remote management of the Server.

1.8 'Line of Business Applications' means the software which is installed on the Managed Equipment and provided by the Customer.

1.9 'MSP Services' means on premise IT support services described in the Service Schedule attached hereto.

1.10 'Local Area Network' ('LAN') means the network infrastructure at the Customer's Site.

1.11 'Managed Equipment' means Servers, Workstations and any other Hardware that is installed or used at the Customer's Site(s) or is listed on the Order and which TMB agrees to support under the terms of this Agreement.

1.12 'Monitoring Agent' means Software which is installed on the Managed Equipment by TMB which enables system monitoring, maintenance and performance reporting.

1.13 'Monitoring Service' means Managed Equipment monitoring and management services.

1.14 'Network Equipment' means a sub-set of Managed Equipment that comprises routers, switches, wi-fi controllers and wi-fi access points.

1.15 'Public Internet' means the world-wide collection of private and public router-based networks that are interconnected via gateways and exchange points.

1.16 'Remote Monitoring and Management' means TMB's system for monitoring Managed Equipment performance and the subsequent resolution of Issues thus identified.

1.17 'Service Component' means a component part of the Services.

1.18 'Service Request' means the Customer's report of an Issue or request for assistance.

1.19 'Server' means Managed Equipment which functions as a server.

1.20 'Service Desk' means TMB's support team.

1.21 'Service Desk Operational Hours' means 9.00am to 5.00pm Monday to Friday, excluding bank and public holidays.

1.22 'Site' means Customer's site at which Managed Equipment is located, as set out in the Order.

1.23 'Software' means the software which is covered by the Service Components listed on the Order.

1.24 'Workstation' means Managed Equipment which functions as a desktop workstation or laptop computer.

2. TERM

2.1 This Agreement will be deemed to come into effect on acceptance of the Customer's Order by TMB and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for the Minimum Term as set out in the Order.

2.2 This Agreement shall continue to run after the expiry of the Minimum Term (or subsequent Additional Term) for an Additional Term. The duration of the Additional Term shall be one year, unless otherwise set out on the

Order. TMB shall, not less than thirty days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Customer of changes to charges and any other changes to the terms of this Agreement.

2.3 In the event that:

2.3.1 The Customer serves notice to terminate this Agreement in accordance with clause 11 of the General Terms and Conditions or clause 9 hereof, this Agreement shall terminate at the end of the calendar month immediately following the end of the Minimum Term or Additional Term thereafter;

2.3.2 The Customer notifies TMB of acceptance of changes, the Agreement shall continue in force for an Additional Term;

2.3.3 The Customer fails to notify TMB of acceptance of changes and fails to serve notice to terminate, such failure to notify TMB shall imply that the changes have been accepted and the Agreement shall continue in force for an Additional Term.

3. PROVISION OF SERVICES

3.1 MSP Services are provided to support the Managed Equipment. MSP Services will be provided by TMB remotely. For the avoidance of doubt, MSP Services do not include the provision or support of network connectivity outside of the Customer's Site(s) unless indicated otherwise on the Order.

3.2 The Services comprise MSP Services as set out in the Order and described in the attached Service Schedule. TMB shall use reasonable endeavours to provide the MSP Services during the hours of cover set out in the Schedule.

3.3 The MSP Services provided shall include those set out in the Order and fully described in the Schedule.

3.4 During the term of this Agreement, TMB shall be entitled to make alterations to the Configuration of the Managed Equipment. Such alterations may result in temporary disruption to the availability of the Managed Equipment and TMB will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

3.5 TMB cannot guarantee and does not warrant that the MSP Services shall result in the Managed Equipment operating free from interruptions or temporary degradation of the quality of the services provided by such Managed Equipment.

3.6 If TMB provides Monitoring Services under the terms of this Agreement:

3.6.1 TMB shall use reasonable endeavours to provide the Monitoring Services 24 x 7 x 365;

3.6.2 TMB cannot guarantee and does not warrant that the Monitoring Services will be free from interruptions, including:

a) Interruption of the Monitoring Services for operational reasons and temporary degradation of the quality of the monitoring services;

b) Interruption of the network connection between the Monitoring Services and the monitored equipment; and

c) Any such interruption of the Monitoring Services referred to in this sub-clause shall not constitute a breach of this Agreement.

3.7 Although TMB will use reasonable endeavours to ensure the accuracy and quality of the Services, the Services are provided on an "as is" basis and TMB does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for purpose of the Services.

4. ACCEPTABLE USE

4.1 The Customer agrees to use the Managed Equipment in accordance with the provisions of this Agreement, any relevant Service literature and all other reasonable instructions issued by TMB from time to time.

4.2 The Customer agrees to ensure that the Managed Equipment is not used by its End Users to:

4.2.1 Post, download, upload or otherwise transmit materials or data which is abusive, defamatory, obscene, indecent, menacing or disruptive;

4.2.2 Post, download, upload or otherwise transmit materials or data uploads or make other communications in breach of the rights of third parties, including but not limited to those of quiet enjoyment, privacy and copyright;

4.2.3 Carry out any fraudulent, criminal or otherwise illegal activity;

4.2.4 In any manner which in TMB's reasonable opinion brings TMB's name into disrepute;

4.2.5 Knowingly make available or upload file that contain viruses, malware or otherwise corrupt data;

4.2.6 Falsify true ownership of software or data contained in a file that the Customer or End User makes available via Managed Equipment;

4.2.7 Falsify user information or forge addresses;

4.2.8 Act in any way which threatens the security or integrity of the Managed Equipment, including the download, intentionally or negligently, of viruses, ransom-ware, Trojan horses or other malware;

4.2.9 Violate general standards of internet use, including denial of service attacks, web page defacement and port or number scanning;

4.2.10 Connect to the Managed Equipment insecure equipment or services able to be exploited by others to carry out actions which constitute a breach of this Agreement including the transmission of unsolicited bulk mail or email containing infected attachments or attempts to disrupt websites and/or connectivity or any other attempts to compromise the security of other users of our network or any other third party system;

4.3 The Customer acknowledges that it is responsible for all data and/or traffic originating from the Managed Equipment.

4.4 The Customer agrees to immediately disconnect (and subsequently secure prior to reconnection) equipment generating data and/or traffic which contravenes this Agreement upon becoming aware of the same and/or once notified of such activity by TMB.

5. CUSTOMER'S OBLIGATIONS

During the term of this Agreement, the Customer shall:

5.1 Pay all additional charges levied by TMB, including those arising from usage-based components of the Services.

5.2 Ensure that user-names, passwords and personal identification numbers are kept secure and wherever reasonably possible, use two-factor authentication for Equipment that is exposed to the Public Internet.

5.3 Agree that in all instances where it attaches equipment that has not been provided by TMB to the Managed Equipment that such equipment shall be technically compatible and conforms to any reasonable instruction issued by TMB in relation thereto.

5.4 Accept that if it attaches equipment that does not comply with the provisions of sub-clause 5.3 ('Unauthorised Equipment') and such Unauthorised Equipment in the reasonable opinion of TMB is causing disruption to the functionality of the Managed Equipment, TMB shall be entitled to:

5.4.1 If technically possible, reconfigure the Unauthorised Equipment, and charge the Customer for its work at its prevailing rates;

5.4.2 Charge the Customer at its prevailing rates for any additional work arising from, or in connection with the Unauthorised Equipment;

5.4.3 Request that the Customer disconnect the Unauthorised Equipment from the Managed Equipment; and if such request is not agreed by the Customer within thirty days, terminate this Agreement forthwith.

5.5 Accept that it is the Customer's sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training to prevent the introduction of viruses and other malware into the Managed Equipment.

5.6 Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the Managed Equipment that has been provided by the Customer.

5.7 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the Managed Equipment.

6. TMB'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Customer of its obligations hereunder, TMB shall:

6.1 Provide the Services set out in the Order and described in the attached Service Schedule.

6.2 During the hours of cover set out in the Order, make available a Service Desk that shall provide support and guidance in the use of the Managed Equipment and manage the resolution of all Managed Equipment-related Issues raised by the Customer.

6.3 During the hours of cover set out in the Schedule or as amended in the Order, provide Monitoring Services.

6.4 Respond to Service Requests and make reasonable endeavours to repair any Issue within the Managed Equipment that is reported either by the Customer or identified by TMB.

6.5 Make reasonable endeavours to repair any Issue that occurs within the Managed Equipment that is directly caused by TMB, its employees, agents, subcontractors or suppliers.

6.6 Proactively respond to Alerts reported by the Monitoring Services and make reasonable endeavours to repair any Issue that arises within the Managed Equipment.

7. INDEMNITIES

7.1 The Customer agrees to indemnify, defend and hold harmless TMB and its suppliers from and against any liabilities, actions, losses damages, judgements, costs, fines, claims or expenses incurred by TMB or legal proceedings which are brought or threatened against TMB by a third party in the event of:

7.1.1 The Managed Equipment being used in breach of the acceptable uses set out in Clause 4 hereof;

7.1.2 The Customer being or having been in breach of sub-clause 5.7 hereof or any applicable laws;

7.1.3 Any fraud except by TMB;

7.1.4 Any claims made by third parties arising from Issues in the Services.

7.2 If TMB becomes aware of any claim as set out in sub-clause 7.1 it shall:

7.2.1 As soon as reasonably practical, notify the Customer of such claim;

7.2.2 Make no admission relating to such claim or legal proceedings without agreement of the Customer, such agreement not to be unreasonably delayed or withheld;

7.2.3 Consult with the Customer regarding the conduct of any action and have due regard for the Customer's representations and not agree any settlement, legal proceedings or make any payment by way of liquidated damages without the prior written agreement of the Customer, such agreement not to be unreasonably delayed or withheld.

7.3 Subject to the limitations in Clause 10 of the General Terms and Conditions, each party (the first party) to this Agreement will fully indemnify and hold harmless the other from any claim or liability whatsoever from a third party arising directly or indirectly from the failure of one of the first parties to obtain or maintain any of the licences, approvals, authorisations or consents as set out in sub-clauses 5.3 and 6.15 of the General Terms and Conditions.

8. GENERAL

8.1 TMB may perform any Planned Maintenance that may limit the availability of the Monitoring Services. Planned Maintenance will be scheduled to minimise disruption to the Customer.

8.2 If the resolution to an Issue or the application of a patch requires the reboot of Servers or Workstations, TMB shall execute the reboot as per the agreed reboot schedule, unless the Customer requests or agrees otherwise.

8.3 TMB will from time to time issue de-support notices against specific older versions of the installed Software product which is installed on the Managed Equipment. Such notices will be issued at least ninety days prior to the notice taking effect. During this period, TMB will provide an upgrade path in consultation with the Customer.

8.4 TMB may be unable to provide prior notice of Emergency Maintenance but will endeavour to minimise the impact of any such maintenance on the Customer.

8.5 If TMB carries out work in response to an Issue reported by the Customer and TMB subsequently determines that such Issue either was not present or was caused by an act or omission of the Customer, TMB shall be entitled to charge the Customer at its prevailing rates.

8.6 If TMB receives notification of a copyright infringement report, a request to provide a copyright infringement list, an order to impose a technical restriction or any other notice, request or order, the Customer will do everything reasonably required by TMB to ensure that both the Customer and TMB will be in compliance with their respective obligations in respect of the provision of the Services.

8.7 Any Equipment or Software that is sold or rented to the Customer by TMB for the purpose of enabling the delivery of the Services set out herein shall be provided subject to the terms of TMB's Supplemental Terms and Conditions for the Sale, Rental or Loan of Goods.

8.8 TMB is responsible for the licensing and installation of the Anti-Virus security software that TMB has installed on the Managed Equipment.

8.9 TMB is responsible for the supply, licensing and installation of Monitoring Agents installed on the Managed Equipment.

8.10 The Customer is responsible for the licensing of all other software, including Windows operating systems, Microsoft Office and Line of Business Applications which have not been supplied by TMB under the terms of any other agreement between TMB and the Customer.

9. TERMINATION

9.1 In addition to the provisions of Clause 11 of the General Terms and Conditions, this Agreement may also be terminated:

9.1.1 By either party by giving the other not less than thirty days notice in writing to terminate at the end of the calendar month immediately following the end of the Minimum Term or any Additional Term thereafter;

9.1.2 By the Customer by giving thirty days notice in writing if TMB makes changes to the terms of this Agreement which are materially disadvantageous to the Customer (for the avoidance of doubt, not including changes to charges) PROVIDED THAT such notice is given within thirty days of the effective date of the change(s).

10. CHARGES AND PAYMENT

10.1 Invoices for periodic charges shall be raised in advance of the relevant period.

10.2 Periodic charges will:

10.2.1 Be based on (a) the number of End Users set out on the Order or subsequently modified by the Customer, (b) the quantity of Managed Equipment that is detected by TMB's Monitoring Service and (c) if applicable, the volume of data backed up by TMB's backup services ;

10.2.2 Include pro-rata charges that reflect changes to the number of End Users, quantity of Managed Equipment and volume of data backup which have occurred during the previous charging period;

10.2.3 Include charges for any ad hoc services provided by TMB during the preceding charging period;

10.2.4 Include charges for rental of Equipment as set out on the Order;

10.2.5 Include additional charges if Servers are do not support Lights Out Management or are not covered by manufacturer's warranty.

10.3 TMB shall commence charging for the MSP Services from the RFS Date, regardless of the date on which the Customer commences use of the MSP Services. If the RFS Date does not correspond with TMB's invoicing period as set out in the Order, TMB shall charge the Customer at a pro-rata rate for the first invoicing period.

10.4 The Customer acknowledges that the charges for the Minimum Term are calculated by TMB in consideration amongst other things of the setup costs to be incurred by TMB and the length of the Minimum Term offered.

10.5 If, during the Minimum Term or Additional Term of this Agreement the Customer requires additional End Users to be added to the Services, the Customer shall raise a change of user request. On receipt of the request TMB shall promptly provide Services to the additional End User(s) and charge the Customer for such additional Services from the date thereof.

10.6 If the Customer requests a reduction in the quantity of Managed Equipment during the Minimum Term:

10.6.1 The Customer shall provide such request in writing, giving TMB not less than thirty days notice;

10.6.2 TMB shall not unreasonably delay its acceptance of the Customer's request;

10.6.3 The Charges for the remainder of the Minimum Term will not be reduced below the amount agreed at the Commencement Date;

10.7 If the Customer requests a reduction in the quantity of Managed Equipment during an Additional Term:

10.7.1 The Customer shall provide such request in writing, giving TMB not less than thirty days notice;

10.7.2 TMB shall not unreasonably delay its acceptance of the Customer's request;

10.7.3 The Charges for the remainder of the Additional Term (and any subsequent Additional Term) will not be reduced below 70% of the amount agreed at the Commencement Date irrespective of the remaining quantity of Managed Equipment;

10.8 The MSP Services will be provided by TMB for use by the Customer on a fair use basis. If, in the reasonable opinion of TMB, the Customer's use of the Services is deemed excessive, TMB and the Customer shall discuss

TMB's concerns and either agree a plan to reduce the excessive use of the Services or agree additional Charges to cover the cost of the excess use of the Services.

10.9 The Customer agrees that it shall be liable for termination charges if this Agreement is terminated by:

10.9.1 The Customer terminating this Agreement for convenience prior to the end of the Minimum Term or any Additional Term, whereupon the Customer shall be liable for the fixed periodic charges payable for the remainder of the current term;

10.9.2 TMB terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Customer's un-remedied breach of the terms of this Agreement, whereupon the Customer shall be liable for the fixed periodic charges payable for the remainder of the current term;

10.10 The Customer shall not be liable for termination charges if this Agreement is terminated by:

10.10.1 The Customer at the end of the Minimum Term or end of any Additional Term PROVIDED THAT the Customer properly serves written notice to terminate, in accordance with Clause 9 of this Supplement and Clause 11 of the General Terms and Conditions;

10.10.2 TMB at any time if it can no longer provide the Services or part thereof;

10.10.3 The Customer by reason of TMB's un-remedied or repeated breach of the terms of this Agreement;

10.10.4 The Customer if TMB makes changes to the Services which detrimentally affect the Customer PROVIDED THAT the Customer complies with the provisions of sub-clause 9.1.2 hereof;

10.10.5 The Customer if TMB makes changes to the terms of this Agreement which are materially disadvantageous to the Customer PROVIDED THAT the Customer complies with the provisions of sub-clause 9.1.2 hereof.

11. LIMITATIONS AND EXCLUSIONS

11.1 The following service limitations shall apply:

11.1.1 Managed Equipment shall be covered by its manufacturer's warranty or third party maintenance contract:

a) If Managed Equipment is not covered by its manufacturer's warranty or a third party maintenance contract, TMB shall be entitled to charge the Customer for any additional parts and / or labour required for Issue resolution; and

b) Firmware upgrades will not be provided by TMB.

11.1.2 Managed Equipment shall have LOM capability and such be enabled and if LOM is not enabled, TMB shall be entitled to charge the Customer for any additional labour required for Issue resolution;

11.1.3 Supported software shall be actively supported by its vendor (that is, not end of life); unsupported versions will be supported by TMB on a reasonable endeavours basis;

11.1.4 TMB shall not provide support for the Customer's Line of Business Applications.

11.1.5 Remediation shall not include the rebuild of operating systems on Servers or Workstations.

11.2 This Agreement and the Services provided by TMB do not include:

11.2.1 The maintenance or support of any Equipment that is not listed on the Order;

11.2.2 Repair or replacement of any damaged Managed Equipment where such damage is caused by accident, misuse or wear and tear;

11.2.3 The supply of any consumables;

11.2.4 Any form of hosting, save backups;

11.2.5 Recovery of Customer data whose loss can be reasonably attributed to accidental deletion, mis-use or negligence by the Customer;

11.2.6 Removal of virus or other malware or the recovery of Customer Data that results from virus or malware infection;

11.2.7 Remediation following a cyber-breach or hack;

11.2.8 Remediation of issues caused by Windows 10 feature upgrades;

11.2.9 Operating system installation or re-installation;

11.2.10 Software installation;

11.2.11 Bare-metal restores;

11.2.12 Third party application or Line of Business Application support;

11.2.13 The provision of development projects;

11.2.14 The provision of End User or 'How to' training;

11.2.15 Support for internet service provider outages;

11.2.16 Power management or UPS support.

TMB may at its sole discretion provide any of the excluded services listed in the sub-clause 11.2, and charge for the supply thereof at its prevailing rates.

11.3 Whilst TMB's Monitoring Service is intended to proactively identify most system-related issues, TMB does not warrant and cannot guarantee that the monitoring system will identify all system-related Issues and shall not be liable for any losses, damages or costs unless such result directly from the negligence of TMB.

11.4 Anti-virus, anti-malware and anti-ransomware services are provided on an 'as is' basis, without warranty, guarantee of fitness for purpose or suitability for the Customer's purpose and TMB shall not be liable for any damage or costs resulting from a failure of an update to the anti-virus or anti-malware software or definitions, or failure to detect a virus or other malware, or incorrect identification of a virus or malware, unless such failure is caused by the negligence of TMB.

11.5 TMB shall not be liable for any damages, costs or charges arising from damage to, or theft of backup data that is transmitted from the Customer's Site to the Data Centre via the Public Internet, nor for any other losses that occur due to reasons beyond its reasonable control.

11.6 Patches are supplied by TMB-authorised software vendors and not TMB. TMB will use reasonable endeavours to prevent a patch causing an adverse reaction with any particular machine configuration, but TMB shall not be liable for any disruption resulting from the installation of patches. In such circumstances, TMB's sole responsibility will be to de-install the patch or roll back to an appropriate restore point to resolve the Issue.

11.7 If a particular component of the Managed Equipment that TMB monitors generates an exceptionally high number of Alerts, such can adversely affect TMB's ability to provide this service to other machines then at TMB's discretion monitoring event logs on the machine will be suspended until the problem is rectified.

11.8 Due to the typically large size of software vendor's service packs TMB will determine the most appropriate method and time of installation to minimise disruption to the Customer. This may require the staged installation of service packs across all Managed Equipment.

11.9 In the event of failure of a Hardware component of the Managed Equipment that is covered by the manufacturer's warranty, TMB shall liaise with the hardware component supplier and manage the replacement and installation of the hardware component, under the terms of the warranty provided by the supplier.

11.10 TMB cannot provide any greater warranty than that offered by the hardware component supplier, and if parts are required that are not covered by the manufacturer's warranty, TMB shall provide the Customer with a quotation for the supply of the replacement part prior to the supply thereof.

Service Schedule

TMB will provide the Service Components that are set out on the Order and described in detail in paragraphs 1 to 11 below. The Services will be provided on a per-End User and / or per device basis, and as set out on the Order.

1. TMB 8 x 5 Service Desk Support

1.1 Subject to fair usage, there are no restrictions on the number of Service Requests that the named End Users can raise with TMB's service desk. TMB's Service Desk provides support, the prompt resolution of Issues and assistance in the use of the Managed Equipment, including the following:

1.1.1 High-Priority Problems

High-priority problems severely impede a client's ability to work. In some cases, multiple users may be affected. Examples include:

- Email or application crashed or not functioning properly
- Printing issues
- File and folder access problems
- General hardware failures
- Computer performance problems
- Virus and malware infections from individual Workstations
- Network connectivity failure on individual Workstations

1.1.2 Administrative Tasks

Administrative tasks include:

- Single user account and group creation
- Mailbox and distribution list creation
- Password resets and unlocking of domain accounts
- File and folder permission changes
- Microsoft Outlook profile set-ups
- Mobile device email setup and configurations along with email, contact, and calendar synchronization troubleshooting
- File and folder restores
- Application of TMB-supplied software licence renewals
- Ongoing documentation maintenance

1.1.3 Microsoft Supported Operating Systems

c) Microsoft operating systems are supported according to the Windows lifecycle fact sheet. Windows 10 must be running a supported feature upgrade.

d) End users are required to be using a supported operating system that is kept up to date with monthly patch releases.

1.1.4 Apple Supported Operating Systems

Latest Mac OS versions (Apple recommends OS based on the compatibility with the desktop/laptop. The Service Desk will support the latest version of Apple OS and the prior two versions).

1.1.5 Office Suites

The Service Desk will support the following versions of MS Office:

- Office 2019
- Office 2016
- Office 365
- Microsoft Office for Mac 2016, 2013, and 2011

1.1.6 Email Clients

The Service Desk will support the following versions of MS Office:

- Microsoft Office 365
- Microsoft Windows Mail App

1.1.7 Browsers

The Service Desk will support the latest version of the following browsers:

- Chrome
- Microsoft Edge
- Microsoft IE
- Firefox
- Safari

1.1.8 Thin Client and Virtual Desktop Interface (VDI)

The Service Desk will provide support for connectivity between Workstations and terminal servers or Citrix servers, subject to both having TMB's Monitoring Agent installed, however Citrix support is provided on a reasonable endeavours basis.

1.1.9 Mobile Devices and Tablets

Device support includes setup and configuration of the default email application and connection to wireless networks The Service Desk will not, however, set up or configure actual devices.

1.1.10 Home Office Support

If a client calling from a home location has a Customer-supplied Workstation with an installed Monitoring Agent, the Service Desk will assist with Customer-related connectivity problems (such as a VPN connection) but will not support other home PC issues.

1.1.11 Third Party Management

TMB will provide hardware failure warranty management and third party vendor liaison.

1.2 TMB will provide a dedicated account manager and a dedicated technical contact for the Customer.

1.3 The Customer shall raise Service Requests by one of the following methods:

1.3.1 Via TMB's client portal, which is accessed from www.tmb.co.uk/customer-login;

1.3.2 By email to TMB's service desk: support@tmb.co.uk;

1.3.3 M1 and P1 Issues (as defined in TMB's Service Level Document) by telephone to TMB's service desk: 0333 900 9050.

1.4 The Service Desk is available to take calls and respond to Service Requests between the hours of 9am to 5.00pm Monday to Friday, excluding bank and public holidays. The Customer may however send emails at any time.

1.5 TMB will raise a Service Request for any Issue it deems necessary during the course of delivering the Services detailed within this Schedule.

1.6 The Service Desk's target initial response and recovery times are set out in paragraph 10 of this Schedule.

1.7 TMB's Service Desk does not include:

- Support for Equipment that does not have TMB's Monitoring Agent installed
- Network device management and configuration (firewalls, routers, switches, etc.). The Service Desk can assist with power-cycling Network Equipment but cannot make configuration changes
- Support for Hardware-related issues (hard disk, memory, power supply, etc.). All hardware and/or equipment issues will be escalated to the Equipment's warranty provider for remediation
- Support for Equipment that has not been fully on-boarded at the commencement of this Agreement
- Onsite Support
- Any excluded services listed in sub-clause 11.2

1.7.1 In exceptional circumstances the Service Desk will install TMB's Monitoring Agent on a Workstation to troubleshoot for a fee of £100 per occurrence. This fee is applied regardless of whether the Service Desk was able to resolve the problem if the technician successfully installed the agent and attempted to resolve the problem.

2. TMB 24 x 7 Service Desk Uplift

If set out on the Order, TMB will extend the hours of cover to 24 x 7 x 365 for the services described in sub-Paragraph 1.1 for one item of Managed Equipment per named End User. Any Issues that TMB are unable to resolve outside of Service Desk Operational Hours will be investigated during the immediately following Working Day.

3. TMB Fully Managed Server Operating System Service

3.1 TMB will install its Monitoring Agents on the agreed Servers to enable pro-active monitoring and maintenance. The Monitoring Agents will monitor key aspects of system performance and will alert TMB to any detected Issues or potential Issues. The Monitoring Agents will monitor Server performance 24 x 7 x 365. TMB shall use reasonable endeavours to remediate any Issues which cannot be automatically remediated during Service Desk Operational Hours in a manner that is appropriate to the severity of the Issue, whilst aiming to minimise disruption to the availability of the Server.

3.2 Hardware maintenance is required to be in place on all Servers that are covered by TMB's Fully Managed Server Operating System Service.

3.3 TMB shall provide the following services:

3.3.1 General Server Support

- Hardware & software audits
- Patch whitelisting service – TMB tests all Microsoft security updates before they are deployed
- Remote restart of services and applications
- Emergency low disk space alerting (Windows & Linux)
- Automated low disk space alert and clean-up (Windows Only)
- AV scan and remediation for infections
- Service Pack Installation outside office hours
- Driver updates
- Firmware updates
- Server Cluster Health Checks and remediation/recommendation for improvement
- Server performance issues, including high CPU usage, high memory usage, memory leaks, and slow response times
- Group policy failures
- Windows server errors

3.3.2 Exchange

- Health checks for Exchange 2003 and above – includes running Best Practice Analyser and fixing issues found
- Defragment and repair Exchange servers
- Update expired web certificates
- Setup email roundtrip monitoring
- Configure recipient update policies for multiple domains

3.3.3 VMware

- Health checks of configurations, including vCPU and memory, network setup
- Review error logs using vSphere or vCenter
- Reconfigure virtual machines & host data stores
- VMware troubleshooting – performance issues on VMs and host machines

3.3.4 Hyper-V

- Health checks including network setup, memory cache, RAID configuration
- Configure virtual machines

- Hyper-V troubleshooting for performance issues

3.3.5 Exchange troubleshooting

- Outlook web or Outlook Anywhere Access
- DAG replication
- Active Sync issues
- Spam
- Auto discovery feature issues
- Restore mailboxes as part of a disaster recovery
- Outlook calendar issues
- Email delivery issues

3.3.6 SBS troubleshooting

- Remote web workspace
- WSUS issues
- Windows Backup issues
- Sharepoint issues
- SBS Console crashes
- Reporting and monitoring services

3.3.7 Remote Desktop troubleshooting

- Login
- Gateway policies
- Web Access
- Single Sign On
- Licensing
- Session issues (including timeout, printing, broken gateway, user profile, certificates)
- Remote Application access
- RDP port

3.3.8 Citrix XenApp Server troubleshooting

- Login
- Secure gateway
- Web access
- Single Sign On
- Licensing
- Session issues, including time out, printing user profile, certificate
- Publish Application, including access, streaming, and publishing issues
- Port
- Load balancing
- XTE Service

3.4 Additional Services Provided During Service Desk Operational Hours.

- The Customer may report any Issues that arise in respect of this service to TMB's Service Desk during Service Desk Operational Hours, using one of the methods described in sub-Paragraph 1.3
- Third party vendor / warranty escalation / management
- On-boarding additional Equipment

3.5 TMB's Fully Managed Server Operating System Service does not include:

- Support for Equipment that does not have TMB's Monitoring Agent installed
- Support for Equipment that has not been fully on-boarded at the commencement of this Agreement
- On-site Support
- Any excluded services listed in sub-clause 11.2

4. TMB Fully Managed Security and Maintenance Endpoint Service

4.1 TMB will install its Monitoring Agents on the agreed Workstations to enable pro-active monitoring and maintenance. The Monitoring Agents will monitor key aspects of system performance and will alert TMB to any detected Issues or potential Issues. The Monitoring Agents will monitor Workstation performance 24 x 7 x 365. TMB shall use reasonable endeavours to remediate any Issues which cannot be automatically remediated during Service Desk Operational Hours in a manner that is appropriate to the severity of the Issue, whilst aiming to minimise disruption to the availability of the Workstations.

4.2 Hardware maintenance is required to be in place on all Workstations that are covered by TMB's Fully Managed Security and Maintenance Endpoint Service.

4.3 TMB shall provide general Workstation management including:

- Proactive Workstation health check and maintenance, including
    - Anti- virus definition checks
    - Workstation performance issues, including high CPU usage, high memory usage, memory leaks, and slow response times
    - Daily temp file cleanup
- Remote Connectivity Agent installation and status checks
- Managed Patching service (Microsoft).
- Third party vendor patching service
- Monthly subscription to TMB Endpoint Security, including anti-virus, anti-malware and anti-crypto protection.
- Remediation of issues with the anti-virus, patching and preventative maintenance functioning
- Monthly reporting on the above.

4.4 Additional Services Provided During Service Desk Operational Hours.

- The Customer may report any Issues that arise in respect of this service to TMB's Service Desk during Service Desk Operational Hours, using one of the methods described in sub-Paragraph 1.3
- Third party vendor / warranty escalation / management
- On-boarding additional Equipment

4.5 TMB's Fully Managed Security and Maintenance Endpoint Service does not include:

- Support for Equipment that does not have TMB's Monitoring Agent installed
- Support for Equipment that has not been fully on-boarded at the commencement of this Agreement
- On-site Support
- Remediation of any Issues that will not be addressed by the services described in Paragraph 4.3
- Any excluded services listed in sub-clause 11.2

5. TMB Network Management Service

5.1 Network Topology maps are automatically generated and maintained along with device configuration backup and configuration change notification & comparison.

5.2 The network management service provides an invaluable troubleshooting capability for identifying issues such as network congestion, broadcast traffic, packet errors and discards along with CPU & memory issues on any managed network device.

5.3 TMB will undertake monthly trend analysis and reporting on the network infrastructure in addition to scheduling annual firmware upgrades for all managed network devices.

5.4 TMB's Monitoring Agent will scan for managed Network Equipment which will automatically be added to the service. This includes managed switches, routers and firewalls. Unmanaged devices will not be added to the service and will not be charged.

5.5 Hardware maintenance is required to be in place on all Network Equipment that is covered by TMB's Network Management Service.

5.6 TMB shall provide the following services:

5.6.1 Network Topology:

- Automated Network Mapping
- Automated Inventory
- Network Documentation
- IP Address Management

5.6.2 Network Monitoring:

- Alerts & Notifications
- Service Monitoring
- Usage & Health Statistics
- Live & Historic Data
- Traffic Insights

5.6.3 Troubleshooting:

- Network Evidence
- Configuration Management
- Configuration Restore
- Configuration Analysis

5.7 Additional Services provided Mon-Fri 09:00 – 17:00

- The Customer may report any Issues that arise in respect of this service to TMB's Service Desk during Service Desk Operational Hours, using one of the methods described in sub-Paragraph 1.3
- Remote analysis of critical network Alerts (such as network device offline)
- Break/Fix support for managed network devices
- Monthly trend analysis including review of alerts generated
- Root cause analysis & attempted remediation of Issues causing service impact
- Monthly exec reporting of managed network devices
- SNMP Configuration of new network devices discovered
- Annual firmware upgrade of managed devices

5.8 TMB's Network Management Service does not include:

- Identifying every device discovered on the network
- Configuring Windows Management Instrumentation
- Wireless security scans for rogue access points or other issues
- Network reconfiguration
- On-site Support
- Any excluded services listed in sub-clause 11.2

6. TMB Unmanaged Server Anti-Virus Client

6.1 TMB will install an industry standard anti-virus and anti-malware product on unmanaged servers as set out on the Order.

6.2 TMB will not monitor anti-virus definition updates on unmanaged servers

7. Service On-boarding

7.1 Prior to commencement of delivery of the Services, TMB shall on-board all Managed Equipment

7.2 TMB will review and where necessary make appropriate changes to the Managed Equipment's configurations to ensure that the Services detailed in this Schedule can be delivered effectively. This will include but is not limited to the configuration of Microsoft Windows event logs, Microsoft Windows, Exchange and SQL Server services, anti-virus software and backup software.

7.3 TMB will carry out a full clean-up of the Managed Equipment, including:

- Application of the latest security patches for operating systems, Microsoft Office and where such applications are listed on the Order, third party applications

- Disk defragmentation
- Removal of unnecessary temporary files, system / application log files, system registry settings, and temporary internet files
- Removal the contents of the recycle bin
- TMB will not remove internet history, recent documents, favourites, cookies, form data or passwords unless specifically requested to do so by the Customer

7.4 TMB will make recommendations about the data that is included or excluded as part of the Customer's backup configuration.

7.5 TMB will agree with the Customer a number of standard procedures that TMB will follow when receiving requests from the Customer for adding, removing or changing access to the Customers network. This will include but is not limited to creating, deleting, or amending user accounts, security permissions, and folders and shares.

7.6 TMB will inform the Customer if TMB is unable to configure any components the Managed Equipment to provide the necessary alerting and will agree a suitable alternative with the Customer.

7.7 TMB will document the Customer's IT infrastructure, identify the roles of each component of the infrastructure and provide the Customer with a copy of the documentation.

8. TMB Office 365 Backup Service

8.1 TMB will back-up the Customer's Office 365 data based on the number of End Users set out on the Order. Backup data is stored on a resilient backup appliance which is located at TMB's EU-based Data Centre.

8.2 Office 365 backups include:

8.2.1 OneDrive file and folder data backups (documents), per End User;

8.2.2 Exchange data, including emails, email attachments, notes, deleted items, contacts (excluding photographs) and calendar events (including attendees, recurrence, attachments and notes);

8.2.3 SharePoint primary, custom, group and team site collections; folders, document libraries and sets; site assets, templates and pages;

8.2.4 Audit logs, data controls and export capabilities.

8.3 Backups will be made three times per day.

8.4 The Customer may initiate additional manual backups at any time.

8.5 The Backup Service is fully managed by TMB.

8.6 The backup system will automatically notify TMB of backup success or failure.

8.7 Backups are encrypted at rest and during transmission.

8.8 TMB will retain backup data as follows:

8.8.1 Each of the three daily backups will be retained for thirty days;

8.8.2 After thirty days one daily backup per user will be retained;

8.8.3 After ninety days one weekly backup per user will be retained;

8.8.4 After one year, one monthly backup per user will be retained;

8.8.5 Data will be retained regardless of whether or not an End User's Office 365 licence is inactivated or deleted.

8.9 Data restoration.

8.9.1 Data restores will only be initiated by TMB when requested by an authorised representative of the Customer;

8.9.2 TMB will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Customer;

8.9.3 TMB will use reasonable endeavours to restore data to the location that is specified by the Customer;

8.9.4 TMB shall charge for executing data restores at its prevailing rates.

8.10 Whilst TMB shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, TMB will carry out the following activities during Service Desk Operational Hours:

8.10.1 Respond to Customer requests for data restores;

8.10.2 Respond to and investigate any Issues that arise in the service which cannot be remediated automatically, whether raised by the Customer or via an Alert received by TMB.

9. TMB Fully Managed 24 x 7 Backup and Disaster Recovery Solution

9.1 TMB will design, document and implement backup and disaster recovery and capacity management policies ('Backup and Disaster Recovery Policy') and install Equipment (as set out on the Order).

9.2 TMB will back-up the Customer's Servers as follows, according to the Backup and Disaster Recovery Policy:

9.2.1 On Customer-supplied hardware located at the Customer's Site; or

9.2.2 On TMB-supplied resilient SBM Appliance located at the Customer's Site.

9.3 If set out within the Order, TMB will additionally back-up the Site-based backup on a resilient backup and disaster recovery appliance which is located at TMB's Data Centre and such backup data storage will be charged per terabyte or part thereof at the rate set out on the Order.

9.4 The Backup and Disaster Recovery Service is fully managed by TMB;

9.5 The backup system will automatically notify TMB of backup success or failure.

9.6 Backups are encrypted at rest and during transmission.

9.7 Incremental Backups are made at the frequency set out within the Backup and Disaster Recovery Policy and initial full backups will be made on commencement of the Services and if deemed necessary by the backup service itself following the reboot of any backed-up Server.

9.8 The data retention period is set out within the Backup and Disaster Recovery Policy.

9.9 Data restoration

9.9.1 Data restores will only be initiated by TMB when requested by an authorised representative of the Customer;

9.9.2 TMB will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level), requested by the Customer;

9.9.3 TMB will use reasonable endeavours to restore data to the location that is specified by the Customer.

9.10 Disaster Recovery

9.10.1 The disaster recovery mode is Active-Passive; In the event of a failure of a Server failure, TMB will discuss a Disaster Recovery plan of action with the customer during TMB working hours and action the plan in accordance with the Customer's instructions;

9.10.2 If the Customer's Server becomes unavailable for use, TMB will either:

a) Initiate failover to a disaster recovery server supplied by the Customer; or

b) Initiate failover to an SBM Appliance at the Customer's Site.

9.10.3 If the Customer's Site becomes unavailable for use, and if set out within the Backup and Disaster Recovery Policy, TMB will initiate failover to a disaster recovery server within its Data Centre and provide temporary access to the Customer's End Users until such time as access to the Site is restored; TMB will make such access available for a maximum of thirty days per annum and any use in excess of thirty days will be chargeable at TMB's prevailing rate.

9.11 The recovery point objective and recovery time objective will be determined by the design of the disaster recovery solution and will be documented within the Backup and Disaster Recovery Policy.

9.12 TMB will use reasonable endeavours to complete the disaster recovery within the recovery time objective documented in the Disaster Recovery Policy.

9.13 TMB shall carry out annual disaster recovery testing. The Customer may, however, request reasonable ad hoc testing as required.

10. TMB Managed Cloud Backup Service

10.1 TMB will design, implement and manage a cloud-based Server backup service.

10.2 TMB will back-up the designated Servers (as set out on the Order) on a resilient backup appliance which is located at TMB's Data Centre and such backup data storage will be charged per terabyte or part thereof at the rate set out on the Order.

10.3 The cloud backup service is fully managed by TMB;

10.4 The backup system will automatically notify TMB of backup success or failure.

10.5 Backups are encrypted at rest and during transmission.

10.6 Incremental Backups are made at the frequency set out on the Order and initial full backups will be made on commencement of the Services and if deemed necessary by the backup service itself following the reboot of any backed-up Server.

10.7 The data retention period is set out on the Order.

10.8 TMB shall in response to requests from the Customer and subject to fair use, restore backup-up data:

10.8.1 Data restores will only be initiated by TMB when requested by an authorised representative of the Customer;

10.8.2 TMB will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level), requested by the Customer;

10.8.3 TMB will use reasonable endeavours to restore data to the location that is specified by the Customer.

11. TMB Unmanaged Cloud Backup Service

11.1 TMB will design and implement a cloud-based Server backup service which will backup the designated Servers (as set out on the Order) on a resilient backup appliance which is located at TMB's Data Centre and such backup data storage will be charged per terabyte or part thereof at the rate set out on the Order.

11.2 The operation of the backup service will not backup service will not be managed by TMB; management of the service shall be the sole responsibility of the Customer.

11.3 Backups are encrypted at rest and during transmission.

11.4 Incremental Backups are made at the frequency set out on the Order and initial full backups will be made on commencement of the Services and if deemed necessary by the backup service itself following the reboot of any backed-up Server.

11.5 The data retention period is set out on the Order.

11.6 TMB shall not be responsible for the restoration of backup-up data.

12. TMB Pre-Paid Day

12.1 TMB's Pre-Paid Days service provides level 1 and level 2 engineering on-site labour. Travel is included in the daily rate.

12.2 Pre-Paid Days can be pre-purchased at the commencement of this Agreement and "topped up" at any time thereafter in blocks of five days which may be called off, with 5 days notice, in minimum units of half a day. Pre-Paid Days cannot be used for project work (for example, design, consultancy or migrations). Pre-Paid Days that have been purchased but not used at the end of the current term will be deemed spent and will not be refundable.

13. TMB Emergency Service Desk Cover

TMB will provide access to the Service Desk Support Service as set out in paragraph 1 on an ad hoc basis to Customers whose subscription to TMB's MSP Services does not include Service Desk Support. The purpose of Emergency Service Desk Cover is to provide assistance on occasions that the Customer's internal IT support is not available. Pre-payment is not required and the Customer will be charged for blocks of fifteen minutes of use. Any period of use that is less than fifteen minutes will be charged as a fifteen minute block. The service does not include on-site support and TMB's SLA will not apply.

14. Service Level Agreement

14.1 TMB's response and recovery targets are documented in TMB's SLA document which can be found at http://www.tmb.co.uk/terms.

14.2 TMB shall make reasonable endeavours to meet the targets set out in TMB's SLA document. Failure by TMB to meet such targets shall not be deemed a breach of this Agreement.

15. Complaint Handling

15.1 If the Customer is dissatisfied with any Services-related matter, the Customer should make a complaint using TMB's escalation process which can be found at http://www.tmb.co.uk/terms