

Supplementary Terms for the Supply of Managed IT Services

The Services set out in these Supplementary Terms shall be supplied by the Company to the Client on the terms and conditions set out in the Company's General Terms and Conditions and the terms and conditions of these Supplementary Terms. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

- 1.1 'Cloud-Based Utilities' means the collection of ancillary third-party provided services, including backup, anti-Malware, and monitoring services which will be used by the Company in support of the Managed IT Services.
- 1.2 'Configuration' means the configuration of the IT Equipment, including hardware, installed software and all associated settings and or parameters.
- 1.3 'Data Centre' means a remote data storage facility.
- 1.4 'Data Security Event' means a breach of the security of the Client's infrastructure resulting in loss or damage, including loss of usernames, passwords, Personal Data; crypto-locking or other Malware-related damage.
- 1.5 'Emergency Maintenance' means any period of maintenance for which, due to reasons beyond its reasonable control, the Company is unable to provide prior notice of.
- 1.6 'Endpoint' means all computing devices save Servers, including desktop computers, laptop computers and mobile computing devices, which collectively form a sub-set of the IT Equipment.
- 1.7 'End User' means a user of the IT Equipment.
- 1.8 'Hosted Services' means Software that is hosted in a Microsoft 365 tenant and accessed by the Client remotely.
- 1.9 'Hours of Cover' means the hours of cover set out in the Service Schedule, unless amended on the Order.
- 1.10 'IT Equipment' means Servers, Endpoints and any other electronic devices that are installed or used at the Client's Site, which are listed on the Order and is/are to be supported under the terms of this Agreement.
- 1.11 'IT Infrastructure' means the IT Equipment, Local Area Network and their respective configuration.
- 1.12 'Local Area Network' ('LAN') means the network infrastructure at the Client's Site.
- 1.13 'Line of Business Application' means the software which is installed on the IT Equipment and is provided by the Client.
- 1.14 'Managed IT Services' means IT support services set out on the Order and described in the Service Schedule.
- 1.15 'Monitoring Agent' means Software which is installed on the Client's Server by the Company which enables system monitoring and performance reporting.
- 1.16 'Planned Maintenance' means any period of maintenance for which the Company provides prior notice.
- 1.17 'Server' means server equipment that is a sub-set of the IT Equipment, which are listed on the Order.
- 1.18 'Service Desk' means the Company's dedicated team of qualified support specialists.
- 1.19 'Service Request' means a request for a Service Component to be actioned, for example adding new End User credentials.
- 1.20 'Site' means Client's site at which IT Equipment is located, as set out in the Order.
- 1.21 'Software' means the software which is installed on the IT Equipment, as listed on the Order.
- 1.22 'Standard Software' means Software including Windows, Microsoft 365 Applications and third-party line of business applications that the Client has covered by active support and maintenance contracts.
- 1.23 'Ticket' means the Client's report of an Incident or a raised Service Request.

2. TERM

- 2.1 This Agreement will be deemed to come into effect on acceptance of the Client's Order by the Company and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for the Minimum Term as set out on 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. In the event that:
 - 2.2.1 The Client 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 Minimum Term or Additional Term thereafter;
 - 2.2.2 The Client notifies the Company of acceptance of changes, the Agreement shall continue in force for an Additional Term;
 - 2.2.3 The Client fails to notify the Company of acceptance of changes and fails to serve notice to terminate, such failure to notify the Company 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 Managed IT Services are provided to support the Client's on-premise IT systems and Hosted Services. Managed IT Services will be provided by the Company remotely and if set out on the Order, when required, visits shall be made to the Client's Site. For the avoidance of doubt, Managed IT Services do not include the provision or support of network connectivity outside of the Client's Site, nor do the Services include maintenance of hardware.
- 3.2 The Managed IT Services to be provided hereunder shall include those set out in the Order and described in the Service Schedule.
- 3.3 During the term of this Agreement, the Company shall be entitled to make alterations to the Configuration of the IT Equipment and / or Hosted Services. Such alterations may result in temporary disruption to the availability of the IT Equipment and / or Hosted Services and the Company will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.
- 3.4 The Company cannot guarantee and does not warrant that the Managed IT Services shall result in the IT Equipment or Hosted Services operating free from interruptions or temporary degradation performance quality.
- 3.5 The Company provides Cloud-Based Utilities under the terms of this Agreement; and:
 - 3.5.1 The Company shall use reasonable endeavours to provide the Cloud-Based Utilities 24 x 7 x 365;
 - 3.5.2 The Company cannot guarantee and does not warrant that the Cloud-Based Utilities will be free from interruptions, including:
 - a) Interruption of the Cloud-Based Utilities for operational reasons and temporary degradation of the quality of the Server Monitoring services;
 - b) Interruption of the network connection between the Cloud-Based Utilities and the IT Equipment; and
 - c) Any such interruption of the Cloud-Based Utilities referred to in this sub-clause shall not constitute a breach of this Agreement.
 - 3.5.3 Although the Company will use reasonable endeavours to ensure the accuracy and quality of the Cloud-Based Utilities, such are provided on an "as is" basis and the Company does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for purpose of the Cloud-Based Utilities.

4. ACCEPTABLE USE

- 4.1 The Client agrees to use the IT Equipment and / or Hosted Services in accordance with the provisions of this Agreement, any relevant Service literature and all other reasonable instructions issued by the Company from time to time.
- 4.2 The Client agrees to ensure that the IT Equipment and / or Hosted Services are 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 the Company's reasonable opinion brings the Company's name into disrepute;
 - 4.2.5 Knowingly make available or upload file that contain Malware or otherwise corrupt data;
 - 4.2.6 Falsify true ownership of software or data contained in a file that the Client or End User makes available via IT Equipment or Hosted Services;
 - 4.2.7 Falsify user information or forge addresses;
 - 4.2.8 Act in any way which threatens the security or integrity of the IT Equipment, Hosted Services or Cloud-Based Utilities, including the download, intentionally or negligently, of 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 IT Equipment or Hosted Services 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 Client acknowledges that it responsible for all data and/or traffic originating from the IT Equipment and /or Hosted Services.
 - 4.4 The Client 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 the Company.
 - 4.5 The Client agrees not to and ensure that its End Users do not share passwords provided for the use of Cloud-Based Utilities.
 - 4.6 Subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, the Client shall indemnify the Company against any third-party claims arising from the Client's breach of the terms of this clause 4.

5. CLIENT'S OBLIGATIONS

- 5.1 During the term of this Agreement, the Client shall:
- 5.2 Pay all additional Charges levied by the Company, including those arising from usage-based components of the Services.
- 5.3 Use reasonable endeavours to ensure that user-names, passwords and personal identification numbers are kept secure and:
 - 5.3.1 On a regular basis, change access passwords for all IT Equipment and / or Hosted Services that in the Client's reasonable opinion may be liable to access by unauthorised persons.
- 5.4 Agree that in all instances where it attaches equipment that has not been provided by the Company to the IT Equipment or Hosted Services that such equipment shall be technically compatible and conforms to any instruction issued by the Company in relation thereto.
- 5.5 Accept that if it attaches equipment that does not comply with the provisions of sub-clause 5.4 ('Unauthorised Equipment') and such Unauthorised Equipment in the reasonable opinion of the Company is causing disruption to the functionality of the IT Equipment, the Company shall be entitled to:
 - 5.5.1 If technically possible, reconfigure the Unauthorised Equipment, and charge the Client for the work at its prevailing rate;
 - 5.5.2 Charge the Client at its prevailing rate for any additional work arising from, or in connection with the Unauthorised Equipment;
 - 5.5.3 Request that the Client disconnect the Unauthorised Equipment from the IT Equipment or Hosted Services; and if such request is not agreed by the Client within thirty days, terminate this Agreement forthwith.

- 5.6 Accept that is the Client's sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training to prevent the introduction of Malware into the IT Equipment or Hosted Services.
- 5.7 Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the IT Equipment that has been provided by the Client.
- 5.8 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the IT Equipment and / or Hosted Services.
- 5.9 During term of this Agreement maintain a level of cyber-breach insurance cover that is appropriate to the risks associated with accidental destruction, damage, loss or disclosure of Client Data; general insurance to cover loss of or damage to the IT Equipment; and
 - 5.9.1 In response to reasonable requests made by the Company, provide evidence to show compliance with this sub-clause;
 - 5.9.2 Not do or omit to do anything which would destroy or impair the legal validity of the insurance;
 - 5.9.3 If the Client suffers a Data Security Event and subsequently requests assistance from the Company, ensure that such request for assistance will not breach the terms of the insurance policy prior to requesting assistance from the Company;
 - 5.9.4 Acknowledge that insurance will not relieve the Client of any liabilities under this Agreement.

6. THE COMPANY'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Client of its obligations hereunder, the Company 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 IT Equipment and / or Hosted Services and manage the resolution of all Incidents raised by the Client.
- 6.3 During the Hours of Cover set out in the Service Schedule or as amended in the Order, monitor the performance of the Servers.
- 6.4 Respond to Tickets and make reasonable endeavours to repair any Incident that is within the IT Equipment, Hosted Services or action a Service Request.
- 6.5 Proactively respond to Incidents reported by the Monitoring Agents and make reasonable endeavours to repair any Incident that is within the IT Equipment or Hosted Services.
- 6.6 During the Run-Up Period, the Company shall carry out pre-service on-boarding services as described in the Service Schedule.
- 6.7 If requested, on termination of this Agreement, the Company shall provide assistance in the orderly transition of the Services from the Company to the Client or its nominated replacement supplier (the 'Exit Assistance'); such Exit Assistance will be chargeable at the Company's prevailing rate and examples of the tasks to be performed include:
 - 6.7.1 Hand-over of server images;
 - 6.7.2 Hand-over of backups of Client Data;
 - 6.7.3 The orderly removal of Client Data from the Company's Infrastructure;
 - 6.7.4 The continuity of delivery of the Services;
 - 6.7.5 The orderly removal of any Monitoring Agents installed by the Company on the Client's Equipment to enable delivery of the Services.

7. Clause Intentionally Unused

8. GENERAL

- 8.1 If the Company carries out work in response to an Incident reported by the Client and the Company subsequently determines that such Incident either was not present or was caused by an act or omission of the Client, the Company shall be entitled to charge the Client at its prevailing rate.
- 8.2 In the event of persistent breach of clause 4.2.8, the Company shall be entitled to:
 - 8.2.1 Charge the Client at its prevailing rate for the removal of Malware;

- 8.2.2 Terminate this Agreement.
- 8.3 The Company may perform any Planned Maintenance that may limit the availability of the Cloud-Based Utilities. Planned Maintenance will be scheduled to minimise disruption to the Client. The Client will be notified at least forty eight hours prior to such Planned Maintenance taking place.
- 8.4 The Company may be unable to provide prior notice of Emergency Maintenance to the Cloud-Based Utilities, but will endeavour to minimise the impact of any such maintenance on the Client.
- 8.5 If the Client suffers a Data Security Event and subsequently requests assistance from the Company, it is the Client's sole responsibility to ensure that such request for assistance will not breach the terms of any cyber-insurance policy that the Client has in place, prior to requesting assistance from the Company; and
- 8.5.1 The Company shall be entitled to charge at its prevailing rate for the provision of such assistance.
- 8.6 If the Client is contacted by the Company and requested to make a change to the Configuration of the IT Equipment or Hosted Services, it is the Client's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.
- 8.7 If the Company resets any passwords during the execution of the Services, it shall be the Client's sole responsibility to change such changed passwords and ensure that such changes are compliant with any security policy that may be in effect.
- 8.8 The Client acknowledges that if it elects not to take advice given by the Company in relation to the security and performance of the IT Equipment or Hosted Services, there may be a resulting risk to the integrity of the IT Equipment or Hosted Services and that the Company shall not be liable for any degradation in integrity resulting from such decision and that any additional costs incurred by the Company resulting there from will be charged to the Client.
- 8.9 The Client agrees not to reverse any security policy changes made by the Company without the prior written consent of the Company (such consent not to be unreasonably withheld or delayed).
- 8.10 The Client hereby consents to the Company and its sub-contractors and suppliers accessing the IT Equipment and Hosted Services, for the sole purpose of providing the Services; and
- 8.10.1 Acknowledges that during the configuration of certain Service Components, the Company, its sub-contractors and suppliers may require global administrative access to the Hosted Services.

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 ninety days' notice in writing to terminate at the end of the Minimum Term or Additional Term.
- 9.1.2 Immediately by the Company in the event that it is so instructed by government or a regulatory body;
- 9.1.3 By the Company if it can no longer provide the Services;
- 9.1.4 By the Client by reason of the Company's un-remedied or repeated material breach of the terms of this Agreement;
- 9.1.5 By the Client if the Company or its supplier makes changes to the Services which materially adversely affect the Client (which for the avoidance of doubt, does not include changes to Charges);
- 9.2 The Company may terminate the provision of any Service Component on written notice in the event that its supplier of such Service Component ceases to provide the Service Component to the Company.
- 9.3 On termination, howsoever caused, the Company shall be entitled to charge a termination fee ('Termination Fee'), which will cover the Company's costs of off-boarding the Client's End Users.

10. CHARGES AND PAYMENT

- 10.1 The Company shall raise invoices as follows:
- 10.1.1 Invoices for Recurring Charges shall be raised in advance of the relevant period and the invoicing period is set out on the Order;
- 10.1.2 Usage-based Charges, including Charges made for use of Services in excess of any pre-paid amounts, will be invoiced in arrears;
- 10.1.3 Invoices for on-boarding Charges will be raised in advance.

- 10.2 The Recurring Charges will be based on the number of End Users and set out on the Order and as amended from time to time.
- 10.3 In addition to Charges contemplated in sub-clause 10.2, the Company shall be entitled to charge the Client for:
 - 10.3.1 The ad hoc supply of any Services that are requested by the Client but not set out on the Order;
 - 10.3.2 Reasonable expenses;
 - 10.3.3 Onsite visits that extend beyond the end of the Working Day;
 - 10.3.4 The Termination Fee, which shall be charged based on the number of End Users supported at the date of notification of termination.
- 10.4 The Company shall commence charging for the Managed IT Services from the RFS Date, regardless of the date on which the Client commences use of the Managed IT Services. If the RFS Date does not correspond with the Company's invoicing period as set out in the Order, the Company shall charge the Client at a pro-rata rate for the first invoicing period.
- 10.5 The Client acknowledges that the Charges for the Minimum Term are calculated by the Company in consideration inter alia of the setup costs to be incurred by the Company and the length of the Minimum Term offered.
- 10.6 If, during the term of this Agreement the Client requires additional equipment to be added to the schedule of IT Equipment, the Client shall raise a supplementary Order to cover the additional equipment and the Company shall promptly provide a quotation for the additional Services.
- 10.7 The Managed IT Services will be provided by the Company for use by the Client on a Fair Use basis. If, in the reasonable opinion of the Company, the Client's use of the Services is deemed excessive, the Company shall be entitled to charge the Client at its prevailing rate for the supply of such Services.
- 10.8 The Client agrees that it shall be liable for Early Termination Charges in the event that this Agreement is terminated by:
 - 10.8.1 The Client terminating this Agreement for convenience prior to the end of the Minimum Term or any Additional Term whereupon the Client shall be liable for the Recurring Charges payable for the remainder of the current term, any outstanding installation Charges and the Termination Fee;
 - 10.8.2 The Company terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Client's un-remedied breach of the terms of this Agreement, whereupon the Client shall be liable for the Recurring Charges payable for the remainder of the current term, any outstanding installation Charges and the Termination Fee.
- 10.9 If the Client terminates this Agreement at the end of the Minimum Term or any Additional Term thereafter in accordance with clause 9, the Client shall be liable to pay the Termination Fee.
- 10.10 The Client shall not be liable for Early Termination Charges if this Agreement is terminated by:
 - 10.10.1 The Client at the end of the Minimum Term or end of any Additional Term PROVIDED THAT the Client properly serves written notice to terminate, in accordance with clause 9;
 - 10.10.2 A right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.5.

11. LIMITATIONS AND EXCLUSIONS

- 11.1 In addition to the terms set out in clause 12 of the General Terms and Conditions, the Company shall also be entitled to suspend the provision of Services, in whole or part, without notice due to the Company being required by governmental, emergency service, regulatory body or other competent authority to suspend Services.
- 11.2 Unless otherwise set out on the Order, this Agreement and the Services provided by the Company do not include:
 - 11.2.1 The maintenance or support of any equipment that is explicitly not supported by the Company;
 - 11.2.2 Repair or replacement of any damaged IT Equipment where such damage is caused by accident, misuse or wear and tear;
 - 11.2.3 The supply of any consumables;
 - 11.2.4 Recovery of Client data whose loss can be reasonably attributed to accidental deletion, mis-use or negligence by the Client;
 - 11.2.5 Removal of Malware or the recovery of Client Data that results from Malware infection;
 - 11.2.6 Remediation following a cyber-breach or hack;

- 11.2.7 Operating system installation or re-installation;
- 11.2.8 Software installation;
- 11.2.9 Bare-metal restores;
- 11.2.10 Third-party application or Line of Business Application support;
- 11.2.11 Support for any Software that is not currently supported by its vendor;
- 11.2.12 The provision of development projects;
- 11.2.13 The provision of End User or “how to” training;
- 11.2.14 Support for internet service provider outages;
- 11.2.15 Power management or UPS support;
- 11.2.16 New installations, projects or relocations;

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

- 11.3 The Company cannot provide any greater warranty than that offered by the IT Equipment's supplier, and if parts are required to fix a failure that are not covered by the manufacturer's warranty, or such hardware is not covered by manufacturer's warranty, the Company's obligation shall be limited to using reasonable endeavours provide the Client with a quotation for the supply of the replacement part and labour required to install the replacement part prior to the supply thereof, and the Company does not guarantee that it will be able to source the replacement part.
- 11.4 Whilst the Company's Monitoring Agents are intended to proactively identify most system-related Incidents, the Company does not warrant and cannot guarantee that the Monitoring Agents will identify all system-related Incidents and shall not be liable for any losses, damages or costs unless such result directly from the negligence of the Company.
- 11.5 Cloud-Based Utilities are provided on an 'as is' basis, without warranty, guarantee of fitness for purpose or suitability for the Client's purpose; and
 - 11.5.1 The Company shall not be liable for any damage or costs resulting from a failure of an update to the antivirus or anti-Malware software or definitions, or failure to detect Malware.
- 11.6 The Company shall not be liable for any damages, costs or Charges arising from damage to, or theft of backup data that is transmitted from the Client's Site to the Data Centre via the Public Internet, nor for any other losses that occur due to reasons beyond its reasonable control.
- 11.7 Patches are supplied by the Company-authorized software vendors and not the Company. The Company will use reasonable endeavours to prevent a patch causing an adverse reaction with any particular machine configuration, but the Company shall not be liable for any disruption resulting from the installation of patches. In such circumstances, the Company's sole responsibility will be to de-install the patch or roll back to an appropriate restore point to resolve the issue.

Service Schedule

This Service Schedule sets out all of the services that will be provided by the Company under the terms of this Agreement.

1. On-boarding

Prior to commencement of the Services, the Company will on-board the Client's IT infrastructure:

- Review and if necessary will advise the Client of changes to the IT Equipment's configuration that are required to ensure that the Services detailed in this Service Schedule can be delivered effectively. This will include but is not limited to the configuration of Microsoft Windows event logs, Microsoft Windows, Outlook and SQL Server services, anti-virus software and backup software
- Install Monitoring Agents, anti-Malware software and inform the Client if the Company is unable to configure any of the IT Equipment to provide the necessary alerting and will seek to agree a suitable alternative with the Client
- Make recommendations about the data that should be included or excluded as part of a backup configuration, but is not responsible for these decisions
- Agree a patching policy
- Agree an authorisation and implementation process for staff joiners, leavers and movers
- Gather and securely store passwords

2. Service Desk

2.1 Subject to fair usage, there are no restrictions on the number of Incidents that the Client can report to the Company's Service Desk. The Service Desk provides support for the IT Equipment and / or Hosted Services, including the following:

- Management of the Company's response to and resolution of Incidents within IT Equipment and / or Hosted Services, as per the Service Level Agreement described in paragraph 3
- Management and auctioning of Service Requests as per the Service Level Agreement described in paragraph 3
- Remote access to facilitate Incident resolution if possible and appropriate
- Escalation management if required in the event of protracted Incident resolution
- Third-party vendor liaison where required
- On-site support:
 - In the first instance, the Company will endeavour to resolve Incidents remotely. However, if the Company determines that an on-Site visit is either necessary or is the most efficient manner to resolve an Incident, the Company will dispatch an engineer to the Client's Site
 - The Company will not unreasonably delay the dispatch of an engineer to the Client's Site
 - On-Site visits will be made during the Hours of Cover
 - Subject to Fair Use, there are no restrictions on the number of on-Site visits that the Company will make to support the IT Equipment if it is not possible to resolve an Incident remotely

2.2 The Client may raise Tickets by one of the following methods:

- Via the Company's web support portal: www.itrm.co.uk
- By Email: service@itrm.co.uk
- By Telephone to the Company's Service Desk: 020 8308 3310

2.3 When raising a Ticket, the Client should provide the following information:

- Name of Client and person reporting the Incident
- Contact telephone number
- Description of the Incident / Service Request
- Description of actions taken prior to the Incident occurring
- Explanation of how the Incident has been diagnosed

- Any other relevant information

2.4 The Service Desk is available from 9am to 5pm Monday to Friday, excluding public holidays and two training days per year. The Company will advise the Client in advance of the training days and on those days Tickets should be raised as usual by telephone (leaving voicemail), email or via the web portal. During training days, the Service Level Agreement will not be affected.

3. Service Level Agreement

3.1 The Company's Service Desk response and recovery targets are:

Type	Description	Target Response Time	Target Resolution Time
Critical Systems	Incidents arising in the Clients Servers, network switches, routers, firewalls and internet services	Four Working Hours	Reasonable endeavours
Standard Systems	Workstations (desktop and laptop), printers, scanners, screens, peripherals, Standard Software	Eight Working Hours	
Service Requests	User administration, permission changes, software configuration	One Working Day	

3.2 The Company shall make reasonable endeavours to meet the targets set out in this paragraph. Failure by the Company to meet such targets shall not be deemed a breach of this Agreement.

4. Automated Infrastructure Monitoring and Maintenance 24 x 7

4.1 The Company will install its Monitoring Agents on the Servers, Endpoints and Hosted Services set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert the Company to any detected or potential Incidents ('Alert'). The Monitoring Agents will monitor Server, Endpoint and Hosted Services performance 24 x 7 x 365 and automatically resolve Incidents whenever possible. The Company shall respond to any Alerts that cannot be automatically resolved during Service Desk Hours of Cover in a manner that is appropriate to the severity of the Alert, whilst aiming to minimise disruption to the availability of the monitored Servers, Endpoints and Hosted Services.

4.2 The Company shall:

- Monitor processor, memory and hard disk usage and performance of all Servers to help to prevent system downtime or performance degradation
- Monitor the critical services that are necessary to help to maintain the effective performance of the Server operating system(s)
- Monitor the Windows event logs against the Company's current list of monitored events (including those which indicate a pending or current hardware failure) to help to prevent system downtime or performance degradation
- Remote access to diagnose and remediate Incidents
- Routine Maintenance
- Maintain group security policy

4.3 The Company will install approved patches for Servers, Endpoints and Hosted Services as they are made available for Microsoft-supported operating systems and applications during the patching window agreed during on-boarding. Where a Server or Endpoint re-boot is required to complete patch installation, this will be performed in agreement with the Client.

5. Backup Monitoring

The Company will monitor the success or otherwise of each the Client's backup jobs on a daily basis and respond accordingly to notifications of failures or exceptions to ensure that the system backups complete as completely as possible.

6. Anti-Malware Service

- 6.1 The Company's Anti-Malware Service is focussed on security and speed. It employs a unique approach to Malware protection and is largely cloud-based. This approach means that its monitoring and detection are carried out with very little performance impact and obviates the need for constant updating of Servers and Endpoints with virus definitions. Using advanced artificial intelligence and machine learning, behaviour-based indicators of attack, exploit blocking and continuously updated threat intelligence, the Company aims to rapidly identify and halt any attacks, with the objective of minimising harm and reducing risk to the Client's Endpoints.
- 6.2 If the Client accidentally introduces Malware onto the IT Equipment, the Company shall remove such Malware. This undertaking is however subject to the provisions of clause 8.2 of these Supplementary Terms.

7. Vendor Management

Subject to Fair Use, the Company will provide third-party vendor liaison, including:

- Liaison with the Client's third-party service suppliers including providers of software, hardware and telecoms services if such suppliers require changes to be made to the configuration of the IT Equipment to investigate or resolve issues with the third-party software or services
- On behalf of the Client manage any warranty claims for malfunctioning IT Equipment that is covered by the manufacturer's warranty. Such management may include the Company carrying out engineering activities on behalf of the manufacturer, however the Company cannot provide any greater warranty than that offered by the hardware manufacturer, and if parts are required that are not covered by the manufacturer's warranty, the Company shall provide the Client with a quotation for the supply of the replacement part prior to the supply thereof.

8. Service Performance Reporting

The Company will provide periodic reports which include:

- Service metrics (Incidents raised, resolved, resolution performance against SLA)
- Patch update status
- Anti-Virus exception reports
- Backup status reporting
- Warranty status reporting
- Bitlocker reports
- Once a year, provide a technology road map and advice on current landscape and technology changes

The frequency of the meetings will be agreed with the Client at commencement of the Agreement.

9. User Administration

The Company will ensure that Server-based End User accounts are at all times properly managed and in response to specific requests made by the Client:

- Activate / deactivate software licences
- Update Microsoft Windows and Azure Active Directories to add / remove or change user accounts
- Set up / remove email accounts, data folders and shares, and the related security permissions
- De-provisioning and re-provisioning existing Endpoints and other devices

This service is provided subject to Fair Use. If in the Company's reasonable opinion use of this service is excessive, the Company will be entitled to charge the Client at its prevailing rate.

10. Loan Equipment

In the event of failure of an item of IT Equipment, the Company will, if reasonably possible, loan replacement Equipment to the Client, for a period of up to twenty days. The Company does not guarantee that any loaned Equipment will be of an identical specification to that which it replaces and shall be entitled to charge rental if the Client requires the Equipment for more than twenty days.

11. Optional Services

11.1 Extended Hours of Cover

If set out on the Order, the Company will provide extended Service Desk Hours of Cover to named End Users, as follows; either:

- 8am until 6pm Monday to Friday, excluding public holidays
- 7am until 7pm Monday to Friday, excluding public holidays
- 24 x 7 x 365 for proactive and reactive support for Critical Systems

12. Escalation Process

12.1 If any Incident remains unresolved, the Client should escalate using the following escalation path. If the Incident remains unresolved, the Client should escalate to the next level in the escalation path.

Escalation Level	Role	Contact Details
1	Service Desk Dispatcher	020 8308 3310
2	Dedicated Account Manager	
3	Service Delivery Manager	
4	Service Delivery Director	
5	Managing Director	