Supplementary terms for the supply of Managed IT Services

The Services set out in these Supplementary Terms shall be supplied by Ingenious to the Client on the terms and conditions set out in Ingenious's General Terms and Conditions and those of 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 Ingenious in support of the Managed IT Services.

1.2 'Configuration' means the configuration of the IT Equipment or component thereof, 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 cyber incident which affects of the security of the Client's infrastructure resulting in loss or damage, including loss of user-names, passwords, Personal Data; crypto-locking or other Malware-related damage.

1.5 'Device' means a tablet or mobile device.

1.6 'Emergency Maintenance' means any period of maintenance for which, due to reasons beyond its reasonable control, Ingenious is unable to provide prior notice of.

1.7 'Endpoint' means all computing devices except Servers, including desktop computers, laptop computers, Hosted Services and mobile computing devices, which collectively form a sub-set of the IT Equipment.

1.8 'End User' means a user of the IT Equipment.

1.9 'IT Equipment' means Servers, Endpoints, network equipment, printers and Software installed at the Client's Site, which is listed on the Order and is to be supported under the terms of this Agreement.

1.10 'Hosted Services' means Software that is hosted in a Data Centre and accessed by the Client remotely.

1.11 'Hours of Cover' means the hours of cover set out in the Service Schedule.

1.12 'Incident Report' means the Client's report to the Service Desk of an Incident.

1.13 'Managed IT Services' means the IT support services set out on the Order and described in the Service Schedule.

1.14 'Line of Business Applications' means the software which is installed on the IT Equipment and provided by the Client.

1.15 'Local Area Network' ('LAN') means the network infrastructure at the Client's Site.

1.16 'Monitoring Agent' means Software which is installed on the IT Equipment by Ingenious which enables system monitoring and performance reporting.

1.17 'Monitoring Services' means Ingenious's server monitoring, desktop monitoring and / or backup monitoring services that remotely monitor the performance of Servers, Endpoints and their operating systems.

1.18 'Network Equipment' means network infrastructure equipment including routers, switches (including VoIP switches and switch stacks), firewalls and controllers.

1.19 'Planned Maintenance' means any period of maintenance for which Ingenious has provided prior notice.

1.20 'Server' means IT Equipment which functions as a server.

1.21 'Service Desk' means Ingenious's dedicated team of support specialists.

1.22 'Site' means Client's Site at which IT Equipment is located, as set out in the Order.

1.23 'Software' means the software which is installed on and is a component of the IT Equipment, as listed on the Order.

2. TERM

2.1 This Agreement shall come into effect on the Commencement Date and shall run 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 the same as the Minimum Term, unless otherwise set out on the Order. Ingenious shall, not less than ninety days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Client of changes to Charges and any other changes to the terms of this Agreement. In the event that:

2.2.1 The Client serves notice to terminate this Agreement in accordance with clause 9 hereof, this Agreement shall terminate at the end of the Minimum Term or Additional Term as appropriate;

2.2.2 The Client notifies Ingenious of acceptance of changes, the Agreement shall continue in force for an Additional Term;

2.2.3 The Client fails to notify Ingenious of acceptance of changes and fails to serve notice to terminate, the changes will be deemed 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 Ingenious 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 (except warranty claim management).

3.2 The Services comprise Managed IT Services as set out in the Order and described in the attached Service Schedule. Ingenious shall use reasonable endeavours to provide the Managed IT Services during the Hours of Cover set out in the Service Schedule.

3.3 During the term of this Agreement, Ingenious shall be entitled to make alterations to the Configuration of the supported IT Equipment and Hosted Services. Such alterations may result in temporary disruption to the availability of the IT Equipment or Hosted Services and Ingenious will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

3.4 Ingenious 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 of the quality of the services provided by such IT Equipment or Hosted Services.

3.5 If Ingenious provides services under the terms of this Agreement which rely upon Cloud-Based Utilities:

3.5.1 Ingenious shall use reasonable endeavours to provide the Cloud-Based Utilities 24 x 7 x 365;

3.5.2 Ingenious 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 Cloud-Based Utilities;

b) Interruption of the connection of the Cloud-Based Utilities to other network services provided either by Ingenious or a third party; 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 Ingenious will use reasonable endeavours to ensure the accuracy and quality of the Cloud-Based Utilities, such Cloud-Based Utilities are provided on an “as is” basis and Ingenious 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 in accordance with the provisions of this Agreement, any relevant Service literature and all other reasonable instructions issued by Ingenious from time to time.

4.2 The Client agrees to ensure that the IT Equipment and 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 Ingenious's reasonable opinion brings Ingenious'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 Client or End User makes available via IT 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 IT 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 IT 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 Ingenious's network or any other third-party system;

4.3 The Client acknowledges that it is responsible for all data and / or traffic originating from the IT Equipment 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 Ingenious.

4.5 Subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, the Client shall indemnify Ingenious against all third-party claims that arise out of the Client's breach of this clause 4.

5. THE CLIENT'S OBLIGATIONS

5.1 During the term of this Agreement, the Client shall:

5.2 Pay all reasonable additional Charges levied by Ingenious, including those arising from usage-based components of the Services.

5.3 Ensure that user-names, passwords and personal identification numbers are kept secure.

5.4 Agree that in all instances where it attaches equipment that has not been provided by Ingenious to the IT Equipment that such equipment shall be technically compatible and conforms to any instruction issued by Ingenious 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 Ingenious is causing disruption to the functionality of the IT Equipment, Ingenious shall be entitled to:

5.5.1 If technically possible, reconfigure the Unauthorised Equipment, and charge the Client for its 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; 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 (where such are not provided by Ingenious under the terms of this Agreement) to prevent the introduction of viruses and other Malware into the IT Equipment.

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 any Cloud-Based Utilities provided by Ingenious.

6. INGENIOUS'S OBLIGATIONS

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

6.1 Provide the Managed IT Services set out in the Order and described in the attached Service Schedule, subject to any service limitations set out in the Order and Service Schedule.

6.2 During the Hours of Cover, make available a Service Desk that shall provide support and guidance in the use of the IT Equipment and Hosted Services and manage the resolution of all IT Equipment-related Incident Reports.

6.3 During the hours of cover set out in the Service Schedule or as amended in the Order, monitor the performance of the IT Equipment and Hosted Services, as far as is enabled by any Monitoring Services.

6.4 Respond to Incident Reports and make reasonable endeavours to repair any Incident that is within the IT Equipment or Hosted Services.

6.5 Proactively respond to Incidents reported by the Monitoring Services and make reasonable endeavours to repair any Incident that is within the IT Equipment or Hosted Services.

7. Clause Intentionally Unused

8. GENERAL

8.1 During the term of this Agreement, the Client's suppliers will provide patches and maintenance releases ('Updates') for applying to the Software supported hereunder.

8.1.1 Ingenious shall, at the commencement of this Agreement agree an individual strategy for the application of Updates; and

8.1.2 The Client accepts that if it requests that Updates are not applied, there may be a resulting risk to the integrity of the IT Equipment and that Ingenious shall not be liable for any degradation in integrity resulting from such request; and

8.1.3 Ingenious shall immediately notify Client when Updates have been applied; and

8.1.4 The Client shall test its applications once the Update has been applied to ensure it has not impacted their services. If an Update has an adverse effect on the operation of the Software, Ingenious will where possible remove the Update, in agreement with the Client;

8.2 If the Client requires Updates to be applied to Line of Business Applications:

8.2.1 The Client shall be responsible for providing full installation instructions including any configuration details to Ingenious in advance;

8.2.2 The Client shall be responsible for notifying Ingenious of the availability of patches and maintenance releases to any Line of Business Applications which Client provides.

8.2.3 Ingenious shall install Updates to Line of Business Applications in response to specific requests from the Client, subject to Fair Use. Ingenious shall be entitled to charge for the provision of this service, if, in its reasonable opinion, the number of requests made for such by the Client is excessive, the installation is complex and requires excessive work or if the Client requests that such service is to be provided outside of the hours of cover set out in the Order.

8.3 Ingenious 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 Ingenious will from time to time issue de-support notices against specific older versions of the installed Software products which form part of the IT Equipment. Such notices will be issued at least ninety days prior to the notice taking effect. During this period, Ingenious will provide an upgrade path in consultation with the Client.

8.5 Ingenious may be unable to provide prior notice of Emergency Maintenance, but will endeavour to minimise the impact of any such maintenance on the Client.

8.6 If Ingenious carries out work in response to an Incident Report and Ingenious subsequently determines that such Incident either was not present or was caused by an act or omission of the Client, Ingenious shall be entitled to charge the Client at its prevailing rate.

8.7 In the event of persistent breach of clause 4.2.8, Ingenious shall be entitled to:

8.7.1 Charge the Client at its prevailing rate for the removal of Malware and data recovery;

8.7.2 Terminate this Agreement.

8.8 If the Client suffers a Data Security Event and subsequently requests assistance from Ingenious, 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 Ingenious.

8.9 If the Client is contacted by Ingenious and requested to make a change to the Configuration of the IT Equipment, it is the Client's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.

8.10 If Ingenious 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.

8.11 If the Client requires additional equipment, software or services from third parties, the provision of such shall be contracted directly between the Client and the third parties and if at the Client's request, Ingenious arranges the same, it shall be as an agent for the Client and Ingenious shall have no liability whatsoever in relation to the third-parties' equipment, software or 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 any Additional Term thereafter;

9.1.2 By Ingenious at any time if it can no longer provide the Services;

9.1.3 By the Client by reason of Ingenious's un-remedied or repeated material breach of the terms of this Agreement;

9.1.4 By the Client if Ingenious or its supplier makes changes to the Managed IT Services which materially adversely affect the Client (which for the avoidance of doubt, does not include changes to Charges).

10. CHARGES AND PAYMENT

10.1 Invoices for Recurring Charges shall be raised in advance of the relevant period and the invoicing period is set out on the Order. Recurring Charges will be based on:

10.1.1 The current number of End Users as determined by Ingenious, based initially on the Order and subsequently data obtained from on the Client's identity provider platform;

10.1.2 The current number of Servers as determined by Ingenious, based initially on the Order and subsequently on the Monitoring Services.

10.2 Ingenious shall make its determination contemplated in sub-clause 10.1 on the date of Ingenious's invoicing cycle; and each End User or Server that is determined in accordance with sub-clause 10.1 shall be charged for a minimum period of one month.

10.3 Invoices for on-boarding Charges, as set out on the Order, shall be raised on commencement of this Agreement.

10.4 Invoices for usage-based Charges, including Charges made for use of Services in excess of any pre-paid amounts and any ad-hoc services provided, will be invoiced in arrears.

10.5 Ingenious shall commence charging for the Managed IT Services from the Commencement Date, regardless of the date on which the Client commences use of the Managed IT Services. If the Commencement Date does not correspond with Ingenious's invoicing period as set out in the Order, Ingenious shall charge the Client at a pro-rata rate for the first invoicing period.

10.6 Ingenious shall be entitled to request payment (either in full or in part) prior to delivery of any ad-hoc services.

10.7 The Client acknowledges that the Charges for the Minimum Term are calculated by Ingenious in consideration inter alia of the setup costs to be incurred by Ingenious and the length of the Minimum Term offered.

10.8 Occasionally, Ingenious may offer the Client a new or enhanced Service Component or replacement Service Component in the event of the existing Service Component being withdrawn by its supplier ('Offer') which may involve a change to the Charges:

10.8.1 If the Client accepts the Offer, Ingenious will deploy the new or enhanced Service Component and alter the Charges to be effective from the date of deployment;

10.8.2 If the Client declines the Offer, provided that the reason for Ingenious making the Offer was not the withdrawal of the Service Component, the Services and Charges will continue without change; however if the Service Component is to be withdrawn, Ingenious will withdraw the Service Component and alter the Charges accordingly.

10.9 The Managed IT Services will be provided by Ingenious for use by the Client on a Fair Use basis. If, in the reasonable opinion of Ingenious, the Client's use of the Services is deemed excessive, Ingenious shall be entitled to charge the Client at its prevailing rate for the supply of such Services.

10.10 The Client agrees that it shall be liable for Early Termination Charges if this Agreement is terminated by:

10.10.1 The Client terminating this Agreement for convenience prior to the end of the Minimum Term or Additional Term, whereupon the Client shall be liable for the Recurring Charges payable for the remainder of the current term, plus any other outstanding or incurred Charges;

10.10.2 Ingenious terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Client's un-remedied material breach of the terms of this Agreement, whereupon the Client shall be liable the Recurring Charges payable for the remainder of the current term plus any other outstanding or incurred Charges.

10.11 The Client shall not be liable for Early Termination Charges if this Agreement is terminated by:

10.11.1 The Client at the end of the Minimum Term or Additional Term thereafter PROVIDED THAT the Client properly serves written notice to terminate, in accordance with clause 9;

10.11.2 If a right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.4.

11. LIMITATIONS AND EXCLUSIONS

11.1 In addition to the terms set out in clause 12 of the General Terms and Conditions, Ingenious shall also be entitled to suspend the provision of Services, in whole or part, without notice due to Ingenious being required by governmental, emergency service, regulatory body or other competent authority to suspend Services.

11.2 Whilst Ingenious's Monitoring Service is intended to proactively identify most system-related Incidents, Ingenious does not warrant and cannot guarantee that the Monitoring Service 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 Ingenious.

11.3 Ingenious shall not be liable for any damage or costs resulting from a failure of an update to anti-Malware software, failure to detect a virus or other Malware or incorrect identification of Malware, unless such failure is caused by the negligence of Ingenious.

11.4 Ingenious 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.

11.5 If a Data Security Event occurs, subject to the provisions of sub-clause 8.6, Ingenious's responsibilities will be limited to replacing any lost data from the latest backup, the removal of Malware and if necessary, the re-installation of software.

11.6 In the event of data loss by the Client (whether caused by a Data Security Event or any other reason), Ingenious's responsibility shall be limited to restoration of the latest backup of the applicable data.

11.7 Ingenious will not provide warranty management for hardware or software components of the IT Equipment that are no longer supported by their vendors.

11.8 This Agreement does not include:

11.8.1 The repair or replacement of any IT Equipment or part thereof that is not covered by its manufacturer's warranty;

11.8.2 Repair or replacement under manufacturer's warranty of any damaged IT Equipment where such damage is caused by accident, misuse or wear and tear;

11.8.3 The supply of any consumables;

11.8.4 Any form of hosting, save backups;

11.8.5 Any form of training;

11.8.6 Maintenance of structured cabling including cabling, patch panels and wall sockets.

Ingenious may at its sole discretion provide any of the excluded services listed in this sub-clause 11.8, and charge for the supply thereof at its prevailing rates.

Service Schedule

This Service Schedule describes all of the Service Components that Ingenious can provide. The individual Service Components to be provided to the Client under the terms of this Agreement are set out on the Order. If, during the term of this Agreement the Client requests Ingenious to provide Service Components that are described in this Service Schedule but not set out on the Order, Ingenious will charge for the provision of the requested Service Components at its prevailing rate.

1. Service Desk

1.1 Subject to fair usage, there are no restrictions on the number of Incident Reports that the Client can raise with Ingenious's Service Desk. The Service Desk provides remote (hands-off) support and assistance in the use of the IT Equipment, including the following:

- Management of the prompt resolution of Incidents within the IT Equipment that are identified by the Client
- Provision of help and guidance in the use and configuration of the IT Equipment
- Remote access to the IT Equipment to facilitate Incident resolution if possible and appropriate
- Escalation management if required in the event of protracted Incident resolution
- Management of Change Requests
- Third-party escalations and management

1.2 The Client shall raise Incident Reports by one of the following methods:

- Via Ingenious's web support app
- Via Email: support@ingenious.co.uk
- By Telephone to Ingenious's Service Desk: 020 3745 6630

1.3 The Service Desk is available from 9am to 5.30pm Monday to Friday, excluding bank and public holidays.

1.4 If set out on the Order, the Service Desk will be available for the extended hours as set out therein.

2. Service Level Agreement

2.1 Ingenious shall aim to make an initial response to the Client's request for assistance within the following timeframes:

Priority	Example	Response Guarantee	Response Target
Critical	Outage affecting all End Users	2 Working Hours	Immediate
High	Department or End User offline	4 Working Hours	Immediate
Medium	Workstation performance issues, for example slow browsing	8 Working Hours	4 Working Hours
Low	New End User setup / maintenance	16 Working Hours	8 Working Hours

2.2 Failure by Ingenious to achieve the targets set out in this paragraph 2 shall not be deemed to be a breach of this Agreement.

3. Complaint Handling

3.1 If dissatisfied with any Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the escalation path.

Escalation Level	Role	Contact Details

1	Service Delivery Manager	020 3745 6632
2	Managing Director	020 3745 6631

3.2 Ingenious will respond to complaints within three Working Days.

Service Components Description

4. Service On-Boarding

At the commencement of the Agreement, Ingenious will On-Board the Client's IT Equipment as described below. Any remedial work that is identified will be chargeable at Ingenious's prevailing rate. Each time a new item of IT Equipment is added by the Client, such IT Equipment will be On-Boarded using the same process as below and the Client will be charged as set out on the Order.

4.1.1 Ingenious will, as part of the On-Boarding process produce documentation of the Client's configuration and how the supplied Services are to be configured ('Agreed Configuration Document'), for example, backup schedules, retention times (if not set out herein), disaster recovery plans.

4.1.2 Ingenious will review and where necessary make appropriate changes to the IT Equipment's configurations 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, Exchange and SQL Server services, anti-virus software and backup software.

4.1.3 Ingenious will make recommendations about the data that is included or excluded as part of the Client's backup configuration, and agree and document the backup configuration.

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

4.1.5 Ingenious will inform the Client if Ingenious is unable to configure any components the IT Equipment to provide the necessary alerting and will agree a suitable alternative with the Client.

4.1.6 Ingenious will document the Client's IT infrastructure; identify the roles of each component of the infrastructure.

4.1.7 In the event that Ingenious is required to carry out remedial work to bring any item of the IT Equipment to the required standard prior to being able to provide support, Ingenious shall be entitled to charge the Client at its prevailing rate for such work.

5. On-site support

Ingenious will as it deems necessary provide on-site support:

- In the first instance, Ingenious will endeavour to resolve Incidents remotely. However, if Ingenious determines that an on-Site visit is either necessary or is the most efficient manner to resolve an Incident, Ingenious will dispatch an engineer to the Client's Site
- Ingenious 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 usage, there are no restrictions on the number of on-Site visits that Ingenious will make to support the IT Equipment if it is not possible to resolve an Incident remotely

6. Strategic Planning Meetings

6.1 Ingenious will undertake periodic Strategic Planning Meetings with the Client's senior management and decision makers, the frequency of which will be as agreed. The meetings will include:

- Assisting with the road-mapping of the Client's IT strategy
- Advising on current landscape and technology changes
- Discussing and understanding any ongoing Incidents with the Client

- Analysing Incidents, checking for patterns to help identify root causes
- Understanding the Client's business requirements to determine recommendations and changes where appropriate

6.2 Ingenious will undertake annual budget review meetings, which will include:

- Offering input to future strategy and budgeting

7. Service Reporting

Ingenious will on request provide reports which include:

- Service metrics (Incidents raised and resolved)
- End Users and active system accounts
- Supported Hardware – asset register
- Patch update status

8. Security Awareness Training

Ingenious's Security Awareness Training includes a number of services which are targeted at increasing staff awareness of cyber security threats and how to mitigate them. Security Awareness Training is a recurring service under which Ingenious will provide:

- Access to a wide range of cyber training materials for all staff
- Regular, randomised staff phishing simulations
- Regular IT security review and reports
- Access to staff security awareness assessments
- Reporting of learner assessments, scorecards, etc
- Additionally chargeable, tailored 'spear-phishing' simulations can be provided at the Client's request

9. Third-Party Liaison

Provided that the Client has in place the appropriate manufacturer's warranty or vendor's support contract, Ingenious will:

- Liaise 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 or other extended warranty. Such management may include Ingenious carrying out engineering activities on behalf of the manufacturer, however Ingenious 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, Ingenious shall provide the Client with a quotation for the supply of the replacement part prior to the supply thereof. Additional Charges may be incurred, for example, for Site visits and the returning of IT Equipment.

10. User Administration

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

- Manage End Users, groups, distribution lists and the granting of access permissions for all systems including M365, Active Directory, SharePoint and Google Workspace
- Activate / deactivate software licences
- 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 Ingenious's reasonable opinion use of this service is excessive, Ingenious will be entitled to charge the Client at its prevailing rate.

11. Server Monitoring and Management

Ingenious will install its Monitoring Agents on the Servers set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert Ingenious to any detected or potential Incidents. The Monitoring Agents will monitor Server performance 24 x 7 x 365 and automatically resolve Incidents whenever possible. Ingenious shall respond to any alerts that cannot be automatically resolved during Helpdesk 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. Ingenious 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 Ingenious'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
- Diagnose and remediate Incidents
- Maintain group security policy
- Maintain End User, hardware and Software asset registers
- Install approved security patches as they are made available for the vendor-supported operating systems and applications listed below:
    - Windows Server operating systems

12. Endpoint Monitoring and Management

Ingenious will install its Monitoring Agents on the Endpoints set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert Ingenious to any detected or potential Incidents. The Monitoring Agents will monitor Endpoint performance and automatically resolve Incidents whenever possible. Ingenious shall respond to any alerts that cannot be automatically resolved during Helpdesk 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 Desktops. Ingenious shall:

- Monitor processor, memory and hard disk usage and performance of all Endpoints 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 Endpoint operating system
- Monitor event logs against Ingenious'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
- Diagnose and remediate Incidents
- Install approved security patches as they are made available for the vendor-supported operating systems listed below:
    - Windows operating systems
    - Apple Desktop operating systems

13. Network Monitoring

Network Monitoring provides a suite of services including monitoring, fault identification, discovery, traffic insights and configuration backup. A Monitoring Agent will be remotely installed by Ingenious onto a Servers or Endpoint that will be operational 24 x 7, which will monitor all compatible Servers, Endpoints and Network Equipment. The service provides the following:

13.1 Network visibility and documentation:

- Discovery and mapping – Helping the Client to understand what is connected to the network and how it's connected
- Map of Network Locations – Helping the Client to visualise the performance and availability of the entire network
- Inventory and documentation – Provides details for every compatible device on the network

13.2 Network mapping and navigation:

- Alert Overlay – All active alerts visualised the network map
- Connection Details – Provides information how each device is connected
- Device Details – Provides access to device details

13.3 Network Monitoring

- Alerts and Notifications – Pre-configured and customisable alerts
- Central logging – Which may be used for root cause analysis of network issues
- VPN Monitoring – Identifies VPN capacity issues
- Internet Connection Check – identifies Public Internet connection issues

13.4 Network Configuration Backup Software

- Configuration Backups – Retain earlier configurations as required
- Configuration Comparison – Assists the Client to in resolving configuration issues

13.5 The service is provided subject to the following limitations:

- Some elements of the IT Equipment may require reconfiguration to render them compatible with the service. Work required and carried out by Ingenious will be charged at Ingenious's prevailing rate
- The service is charged based on the number of items of Network Equipment that the service discovers in any month; however charging is subject to a minimum of twenty items of Network Equipment and if less than twenty items are discovered, the minimum Charge will apply
- Installation and configuration of the service will be carried out during the Working Day

14. Endpoint Compliance Monitoring

Ingenious will install its Monitoring Agents on the IT Equipment to enable pro-active monitoring for Endpoint compliance. The Monitoring Agents will monitor Endpoints to check that they are running with the security configuration the Client has advised should be implemented, including disk encryption, AV deployed and active and inactive screen locking. The service will report any non-compliance issues that may affect Endpoint security, which Ingenious shall respond to during Helpdesk Hours of Cover.

15. Managed Firewall

Ingenious's Managed Firewall service includes helps to secure the Client's IT Infrastructure by stopping known threats in near real time and at the same time enabling secure access for remote employees. Ingenious provides ongoing management of the firewall including:

- Security Updates to firmware and software to maintain security levels
- Managing access in response to Client requests
- Changes to rules in response to Client requests
- Filtering website access; allowing the Client to selectively block End User access to specified websites
- Changes to setup, including unblocking websites, making exceptions for users and individual Devices in response to Client requests

16. Mobile Device Management

Ingenious's Mobile Device Management service provides administration and maintenance of the Client's mobile devices. Device management is a critical component of the Client's security strategy: It helps ensure that devices are secure, up-to-date, and compliant with the Client's policies, with the goal of protecting the Client's network and data from unauthorised access. Mobile device management includes:

- Enrolment of devices and End Users
- Publishing security settings, certificates and profiles to devices
- Resource access control
- Monitoring and management, including measuring and reporting device compliance and app inventory
- Publishing mobile apps to devices
- Configuration of email applications

- Securing and removal of corporate data

Mobile device management does not include the publishing or management of anti-Malware software or hardware support for physical devices.

17. Email Signature Management

Ingenious will provide access to a centralised email signature management service for Microsoft 365/Exchange Online subscribers. The service is intuitive to use and guarantees consistency and accuracy of email signature information. The service delivers:

17.1.1 The addition of a full, dynamic, professional email signature to every email sent from any item of the IT Equipment that sends via Microsoft 365/Exchange Online.

17.1.2 A management console which the Client can use to customise email signature layout, including:

- The layout of the signature
- Disclaimer messages
- Promotional banners
- Social media icons
- Photographs of End Users

17.1.3 Any design work requested by the Client will be charged at Ingenious's prevailing professional services rates.

18. Multi-Factor Authentication for Microsoft 365 and Azure

Multifactor authentication adds a layer of protection to the End User sign-in process. When accessing accounts or applications, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone. Ingenious will advise the most appropriate implementation and on agreement with the Client will configure, manage and enforce the authentication process for hosted Microsoft 365 Services and Azure.

19. Cloud Backup for Microsoft 365

19.1 Ingenious will perform a daily backup of the Client's Microsoft 365 tenant and store the backup elsewhere in the cloud. The backup data can be stored in Ingenious's Data Centre or at a Data Centre of the Client's choice.

- Daily backup data includes: OneDrive, Exchange, SharePoint and Teams data
- The service is fully managed by Ingenious
- Ingenious will be alerted if any attempted backup fails

19.2 There are no limits on retention period or amount of data to be backed up.

19.3 In response to specific requests from the Client, and subject to Fair Use, Ingenious will restore data from backups:

- Recovery will be attempted from the available recovery points, but recoverability on specific recovery points may not always be available
- The integrity of the backup container file is checked automatically by the service, however Ingenious cannot guarantee that the files, directories and/or block level items within the container will operate when recovered as required
- Recovery will be carried out during the Working Day

19.4 Recovery testing is available on request and is chargeable at Ingenious's prevailing rate.

19.5 The service is charged per Microsoft 365 user, either active or archived. Ingenious will continue to back up archived users until requested to delete the archived data. An active user will become an archived user when Ingenious is requested to remove an active Microsoft 365 licence.

20. Ingenious Backup for Servers

20.1 This section describes various options (for example, schedule, retention time, backup location) that are available to the Client. The options will be agreed during the On-Boarding process and documented in the Agreed Configuration Document.

20.2 Ingenious will perform scheduled backups of the Client's Endpoints and Servers and store the backup in one or more locations:

- Ingenious's Data Centre
- Local backup appliance either provided by the Client or Ingenious
- Local backup appliance and Ingenious's Data Centre
- Client's Data Centre

20.3 The service is fully managed by Ingenious.

20.4 Ingenious will be alerted if any attempted backup fails.

20.5 Backup data will be consolidated according to the agreed retention schedule.

20.6 In response to specific requests from the Client, and subject to Fair Use, Ingenious will restore data from backups:

- Recovery will be attempted from the available recovery points, but recoverability on specific recovery points may not always be available
- Recovery options include image, folder and file level

20.7 Recovery testing is available on request and is chargeable at Ingenious's prevailing rate.

20.8 Limitations:

- The integrity of the backup container file is checked automatically by the service, however Ingenious cannot guarantee that the files, directories and/or block level items within the container will operate when recovered as required
- Recovery will be carried out during the Working Day

20.9 Recovery testing is available on request and is chargeable at Ingenious's prevailing rate.

20.10 This service will be charged as set out on the Order.

21. Disaster Recovery Planning

Ingenious will provide consultancy and advice in respect of the development and maintenance of a robust disaster recovery plan to ensure business continuity in the event of a major outage.

22. Dark Web Monitoring

End User's credentials are regularly hacked and are made available on the dark web for sale. Ingenious's dark web monitoring service continually scans the dark web for the Client's End User's credentials on an ongoing basis and will raise an alert if any credentials that contain the Client's domain name appear for sale, enabling the Client to take action to change any passwords that may have been the same or similar to the compromised passwords.

23. External Vulnerability Monitoring

Ingenious's External Vulnerability Monitoring monitors open firewall and router ports for potential security exposure. By reporting open ports connected to services including remote desktops, Windows file sharing, SQL Server databases, etc. it is possible to identify potential external vulnerabilities and address them. The report generated by the External Vulnerability Monitoring service shows each scanned IP address, protocol and port numbers, the last time it was queried by External Vulnerability Monitoring service and (if available) the service running on a particular port. By scanning regularly, it is possible for Ingenious to identify any configuration changes or unexpected activity that may otherwise go unnoticed. Whilst any open port can be an attack surface, such are often required to provide necessary services to the Client. The External Vulnerability Monitoring service provides visibility so that ports can be open in a secure and appropriate manner.

24. DNS Filtering

Utilising advanced DNS filtering technology, Ingenious's service ensures that the Client's Devices are protected both on and off the corporate network against various online threats, including Malware, ransomware, phishing attacks, and botnets. DNS Network and Endpoint Security actively blocks access to malicious websites and domains, preventing End Users from inadvertently visiting harmful sites or falling victim to phishing attempts. This helps safeguard the Client's network and sensitive data from cyber threats.

Ingenious provides customisable content filtering policies, allowing the Client to control access to specific categories of websites based on the Client's needs and compliance requirements. The service ensures optimal performance and reliability by utilising a global network of servers strategically located to minimise latency and maximise uptime which helps improve the overall browsing experience for End Users while ensuring that DNS requests are processed quickly and efficiently. Detailed reporting and analytics features allow the Client to gain insights into its internet usage and security posture and to monitor DNS activity, track blocked requests and identify trends in web traffic to better understand and address potential security risks.

25. Zero Trust Endpoint Security

Ingenious's Zero Trust Endpoint Security service provides a suite of services that are designed to mitigate risk of cyber attack to the Client's IT Infrastructure.

25.1 By defining how applications can interact with each other, and by controlling what resources applications can access, such as networks, files, and registries, Ingenious Zero Trust Endpoint Security helps to prevent file-less Malware and software exploits, including:

- Protecting data from malicious behaviour
- Preventing file-less Malware and limit damage from application exploits
- Defining how applications integrate with other applications
- Preventing applications from interacting with other applications, network resources, registry keys, and files
- Preventing applications from interacting with built-in tools such as PowerShell, Command Prompt and RunDLL
- Preventing built-in tools from accessing file shares

25.2 Application allow-listing has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, application allow-listing provides control over which software, scripts, executables, and libraries can run on the Client's IT Infrastructure. This approach not only stops malicious software, but it also stops other unpermitted applications from running and therefore mitigates cyber threats.

25.3 Storage protection provides an advanced storage control solution that protects information by enabling the Client to control the flow and access of data. The Client can choose what data can be accessed, or copied, and the applications, users, and Devices that can access the data. Storage control allows the Client to:

- Choose how data is accessed
- Visualise a full audit of all file access on USB, Network, and Local Hard Drives
- Restrict or deny access to external storage, including USB drives, network shares, or other devices
- Approve for a limited amount of time or permanently
- Restrict access to specific file types
- Limit access to a Device or file share based on the application
- Enforce or audit the encryption status of USB hard drives and other external storage

25.4 Elevation control enables End Users to run selected applications as a local admin and remove local admin permissions without stopping productivity. Elevation control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their End Users, whilst allowing them to run individual applications as an administrator. Key Capabilities of Elevation control include:

- Providing complete visibility of administrative rights
- Providing the ability to approve or deny an End User's administrator access to specific applications within an organization even if the End User is not a local administrator
- End Users can request permission to elevate applications and add notes to support their requests
- Allows setting durations for how long End Users are allowed access to specific applications by granting either temporary or permanent access

26. Anti-Virus

Ingenious's advanced Anti-Virus 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 compared with other anti-virus solutions and obviates the need for constant updating of Servers and Endpoints with virus definitions. The service includes:

- Real-time threat protection
- Ransomware protection
- Anti-phishing filter

27. Centralised Event Log Retention and Analysis (SIEM)

Threat detection requires deep analysis of the large number of log files that are created by the Client's IT systems. Ingenious's Centralised Event Logs and Retention service provides cloud-based automated analysis of system log files and generation of alerts in the event that a threat is discovered. The service leverages machine learning which is based on ever-expanding experience and industry-based threat intelligence feeds. The service provides threat visualisation via a dashboard and reporting.

28. Mobile Security

Ingenious's Mobile Security service gives the Client direct insight into the threats that can affect its employees' mobile devices. The service protects both Android and iOS devices and the cloud-based dashboard that provides immediate visibility and analysis of mobile-borne threats. The service works either in standalone mode or layered on a Mobile Device Management service. The service provides a privacy-friendly, lightweight security app for iOS and Android that helps to block mobile threats before they can harm the Client's business.

Features of the service include:

- Quick and easy set up with zero-touch deployment and one-touch enrolment for MDM-managed devices.
- App and device threats that are monitored (Android) include:
    - Malware
    - Screen recording
    - Leaky apps
    - Camera/Microphone access
    - App permission abuse
    - OS exploits
    - Vulnerable configuration
- Network threats that are monitored (Android & iOS) include::
    - Man-in-the-Middle at tacks
    - Phishing
    - Malicious proxies
    - Malicious web scripts
    - Unsecured Wi-fi
    - Weak Wi-fi security

29. Email Threat Protection

Email Threat Protection provides multilayered filtering that permits legitimate email while automatically blocking malicious threats such as phishing, impersonation, Malware, ransomware, and spam-type messages. The multi-layer filtering engine delivers an extraordinary level of accuracy that reduces both false negatives and false positives. Features include:

- Ease of use – simple and intuitive
- High catch rate resulting in low quarantine management requirements
- Easy to use portal
- Mobile access
- Dashboards for intuitive management
- At-a-glance updates on threats and highly-targeted End Users
- Message retraction for Microsoft 365
- Attachment quarantine

- Link protection rewrites all links to safe versions

30. Email Encryption

Ingenious's Email Encryption service scans the content of all of the Client's outbound email and automatically encrypts or takes action based on Client-specified policies. Features include:

- Automatic, bi-directional email encryption
- Simplified implementation
- Policy-based email protection and data loss prevention
- Automated key management
- Simple, policy-based TLS with secure fail-over
- Convenient interface for senders and recipients
- Multiple secure delivery options
- Flexible delivery: pull or push
- Intelligent, policy-based management
- Robust compliance filters
- Dashboards and over 30 reports
- Proof of compliance
- Continuous updates

31. Email Continuity

Ingenious's Email Continuity provides failsafe protection for the Client's email service at all times, running on a cloud-based redundant secondary server architecture which provides a twenty one day rolling backup. If the Client's primary mail server experiences an outage, all inbound messages are spooled to the cloud-based mail server until the primary mail server is back online. During the outage, End Users can access the last twenty one days' inbound messages and continue to send and receive messages from a backup mailbox. Features include:

- Unlimited data storage for up to twenty one days
- Anti-spam and anti-virus filtering
- Comprehensive reporting
- Real time spool summary

32. Email Archiving

Ingenious's Email Archiving service securely stores emails, attachments, while preserving metadata. Features include:

- eDiscovery or compliance options available depending upon business need
- Easy online access to the Client's message archives
- Effective in encrypted environments and supports regulatory requirements
- Works seamlessly with Office 365, Exchange and other email platforms
- Secure, centralised, off-site storage
- Online access to current and historical messages
- Rapid search and retrieval via full text indexing and search engine technology
- Searches on messages, headers and attachments
- Messages are serialised and time/date-stamped
- Importation of legacy email to unified archive
- Meets stringent compliance and audit rules including SEC, NASD, IDA, HIPAA, SOX, GDPR, FRCP
- Advanced dual encryption to ensure privacy, confidentiality, and non-disclosure
- Full audit trails and reports on email history

- Secure offsite storage with multi-data centre replication
- Complete life cycle management with variable retention and disposal periods