Supplementary terms for the supply of Hosted IT Support 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 those of these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

1.1 'Configuration' means the configuration of the IT Equipment or component thereof, including hardware, installed software and all associated settings and or parameters.

1.2 'Data Centre' means a remote data storage facility.

1.3 'Data Security Event' means a breach 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.

1.4 'Domain Name' means a unique name that identifies a website or other services that communicate via the Public Internet.

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 a workstation, laptop, tablet or other device which is used to access the Hosted Services.

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

1.8 'IT Equipment' means servers and Endpoints installed at the Client's Site, which is listed on the Order and is to be supported under the terms of this Agreement.

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

1.10 'IT Support Services' means the IT support services to be provided hereunder which are set out on the Order and described in the Service Schedule.

1.11 'Hosted Services' means cloud-based Microsoft 365 and Azure services.

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

1.13 'Malware' means software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system, including Trojan horses, viruses and ransomware.

1.14 'Microsoft' means Microsoft Corporation; the vendor of the Subscription based Hosted Services.

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

1.16 'Monitoring Services' means the Company's Endpoint monitoring services that remotely monitor the performance of Endpoints and their operating systems.

1.17 'Planned Maintenance' means any period of maintenance for which the Company has provided prior notice.

1.18 'Services' means IT Support Services and Hosted Services.

1.19 'Service Desk' means the Company's dedicated team of support specialists.

1.20 'Service Request' means a requirement for a change to the configuration of the Hosting Services or IT Equipment.

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

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

1.23 'Subscription' means a subscription to a single licence to use the Hosted Services.

1.24 'Ticket' means the report of an Incident or Service Request to the Company by the Client.

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 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 twelve months, unless otherwise set out on the Order. The Company 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 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 The Services comprise Hosted Services and IT Support Services.

3.2 If set out on the Order, the Company will enable the provision of Hosted Services:

3.2.1 The Hosted Services are provided under Subscriptions directly by the Microsoft and comprise the following Service Components:

a) Microsoft 365 online applications;

b) Microsoft 365 online services;

c) Microsoft Azure.

3.2.2 The specific Service Components to be provided under the terms of this Agreement are set out on the Order;

3.2.3 The Subscriptions will be managed on behalf of the Client by the Company;

3.2.4 The Client acknowledges that the Hosted Services will be provided directly to the Client by Microsoft;

3.2.5 The Client hereby appoints the Company as its agent for the purposes of registering the Client's subscription to the Hosted Services, maintaining the Client's subscription to the Hosted Services and billing the Client for the subscription to the Hosted Services; and

a) Authorises the Company to subscribe to the Hosted Services set out on the Order and described in the Service Schedule, on its behalf; and

b) Agrees to at all times comply with and be legally bound by the terms of Microsoft's prevailing licence and / or service terms for the use of the Hosted Services; and

c) Acknowledges that it is the Client's sole responsibility to obtain a copy of such terms and conditions and to comply therewith; and

d) Agrees that any breach by the Client of Microsoft's terms and conditions shall be deemed a breach of this Agreement.

3.2.6 In respect of any Domain Name that the Client supplies to be linked with email hosting components of the Hosted Services, the Client confirms and warrants that it is the owner of or that it has been licensed by the owner to use, any relevant trademark or name as the domain name and subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, indemnifies the Company against all third-party claims and proceedings arising from infringement of any Intellectual Property rights of any third party in relation to the Domain Name;

3.2.7 The Company does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for the Client's purpose of the Hosted Services.

3.3 The Company will provide IT Support Services:

3.3.1 IT Support Services are provided to support the Hosted Services and the IT Equipment. For the avoidance of doubt, IT Support Services do not include the provision or support of network connectivity outside of the Client's Site (as required for access to the Hosted Services), nor do the Services include maintenance of hardware, save warranty management and engineering activities that result there from;

3.3.2 The IT Support Services as set out in the Order and described in the attached Service Schedule. The Company shall use reasonable endeavours to provide the IT Support Services during the Hours of Cover set out in the Service Schedule;

3.3.3 During the term of this Agreement, the Company shall be entitled to make alterations to the Configuration of the Hosted Services. Such alterations may result in temporary disruption to the availability of the 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;

3.3.4 The Company cannot guarantee and does not warrant that the IT Support Services shall result in the IT Equipment or Hosted Services operating free from interruptions or temporary degradation of performance.

4. ACCEPTABE 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 the Company 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 the Company's reasonable opinion brings the Company's name into disrepute;

4.2.5 Knowingly make available or upload file that contains 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 the 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 or Hosted Services, 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;

4.2.11 Send email to anyone who does not wish to receive it.

4.3 The Client acknowledges that it responsible for all data and / or traffic originating from the IT Equipment and 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, subject to the provisions of sub-clause 10.13 of the General Terms and Conditions to indemnify the Company against all costs, damages, expenses or other liabilities arising from any third-party claim which arises from the Client's breach of this clause 4.

5. THE CLIENT'S OBLIGATIONS

During the term of this Agreement, the Client shall:

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

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

5.3 Accept that if it attaches equipment that does not comply with the provisions of sub-clause 5.2 ('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:

5.3.1 If technically possible, reconfigure the Unauthorised Equipment, and charge the Client for its work at its prevailing rate;

5.3.2 Charge the Client at its prevailing rate for any additional work arising from, or in connection with the Unauthorised Equipment;

5.3.3 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.

5.4 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 the Company under the terms of this Agreement) to prevent the introduction of Malware into the IT Equipment and Hosted Services.

5.5 Be solely responsible for ensuring compliance with the terms of licence of any Software that is installed on the IT Equipment that has been provided by the Client.

5.6 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the IT Equipment and the Hosted Services.

5.7 Prior to commencement of the Services, ensure that all IT Equipment:

5.7.1 Is enrolled into Microsoft InTune;

5.7.2 Has Microsoft 365 defender for Endpoints installed;

5.7.3 Is running Windows 10 or higher;

5.7.4 Has Microsoft TeamViewer installed.

5.8 Permit the installation by the Company of its Monitoring Agents on all IT Equipment.

5.9 Provide the Company with global administrator access permissions.

5.10 Shall use the Hosted Services in accordance with the provisions of Microsoft's terms and conditions of use, this Agreement, any relevant service literature and all other reasonable instructions issued by the Company or Microsoft from time to time.

5.11 Shall ensure that user-names, passwords and personal identification numbers are kept secure and:

5.11.1 On a regular basis, change access passwords for all equipment that in the Client's reasonable opinion, may be liable to access by unauthorised persons;

5.11.2 Change passwords as appropriate when employees leave;

5.11.3 Use strong passwords;

5.11.4 Immediately notify the Company in the event that, or there is reasonable suspicion that such information has become known to any unauthorised person;

5.11.5 Acknowledge that the Company shall be entitled to temporarily suspend the Hosted Services and / or change the Client's passwords in the event that in the Company's reasonable opinion, unauthorised persons may have access to the Hosted Services.

5.12 Shall be solely responsible for the configuration of its internal local area network, and connection to the Public Internet and agree that any interruption in or to the Hosted Services which result from the configuration of the Client's local area network or connection to the Public Internet shall not be regarded as interruption in or suspension of the Hosted Services provided by the Company.

5.13 Promptly report to the Company any Incident that arises in the Hosted Services.

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, 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- and Hosted Services-related 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 IT Equipment.

6.4 Respond to Tickets raised by the Client and make reasonable endeavours to repair any Incident that is within the IT Equipment or Hosted Services or is directly caused by the Company, its employees, agents, subcontractors or suppliers.

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.

6.6 Register and maintain the Client's Subscriptions to the Hosted Services set out in this Agreement, subject to any service limitations set out in the Order and Service Schedule.

7. Clause Intentionally Unused

8. GENERAL

8.1 The Company may perform any Planned Maintenance that may limit the availability of the Hosted Services. 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.

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

8.3 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.

8.4 In the event of persistent breach of clause 4.2.8, the Company shall be entitled to:

8.4.1 Charge the Client at its prevailing rate for the removal of Malware;

8.4.2 Terminate this Agreement.

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.

8.6 If the Client is contacted by the Company 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.

8.7 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 in 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 hereby consents to the Company and its sub-contractors accessing the IT Equipment and Hosted Services, for the sole purpose of providing the Services.

8.10 If the Company receives notification of a copyright infringement report, a request to provide a copyright infringement list, an order to impose a technical restriction or any other notice, request or order, the Client will do everything reasonably required by the Company to ensure that the Company and the Client will be in compliance with their respective obligations in respect of the provision of 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 any Additional Term thereafter;

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

10. CHARGES AND PAYMENT

10.1 Invoices for fixed periodic Charges shall be raised in advance of the relevant period. The invoicing period is set out in the Order.

10.2 Invoices for additional services will be raised in arrears.

10.3 The Company shall commence charging for the Services from the RFS Date, regardless of the date on which the Client commences use of the 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.

10.4 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.

10.5 If, during the Minimum Term or Additional 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.

10.6 The Client may at any time during the term of this Agreement, by raising a supplemental Order purchase additional Subscriptions and acknowledges that at the price quoted by the Company for such additional Subscriptions may differ from any previous Subscriptions purchased or quotations provided by the Company.

10.7 During any term of this Agreement, the Client may decrease the number of Subscriptions, PROVIDED THAT such provision is set out on the Order and subject to any limitations thereto as set out on the Order.

10.8 The IT Support 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 and the Client shall discuss the Company's concerns and either agree a plan to reduce the excessive use of the Services or agree additional Charges to cover the cost of the excess use of the Services.

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

10.9.1 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 fixed periodic Charges payable for the remainder of the current term;

10.9.2 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 fixed periodic Charges payable for the remainder of the current term.

10.10 The Client shall not be liable for 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 of these Supplementary Terms;

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

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

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

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

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

11.3 The Company shall not be liable for any remedial work, damages, costs or charges resulting from:

11.3.1 The failure of an update to anti-Malware software, failure to detect Malware or incorrect identification of Malware, unless such failure is caused by the negligence of the Company;

11.3.2 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;

11.3.3 Incidents that arise directly from the failure of the Client to implement recommendations and / or advice provided by the Company.

11.4 The Services provided by the Company under the terms of this Agreement are solely IT Support Services and do not include:

11.4.1 The resolution or remediation of consequences of Data Security Events;

11.4.2 The investigation of the causes of Data Security Events.

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

11.6 The Company will not provide warranty management for hardware components of the IT Equipment that are no longer supported by their vendors.

11.7 This Agreement does not include:

11.7.1 The support of any equipment that is not listed on the Order;

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

11.7.3 The supply of any consumables;

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

11.7.5 The recovery of Client's data that results from Malware infection;

11.7.6 Maintenance of structured cabling including cabling, patch panels and wall sockets;

11.7.7 Connection of the Client's Site to the Public Internet or Hosted Services;

11.7.8 The installation of Software at the Client's Site;

11.7.9 The pre commencement of service obligations listed in sub-clause 5.7;

11.7.10 Web-site hosting;

The Company may at its sole discretion provide any of the excluded services listed in this sub-clause 11.7, and charge for the supply thereof at its prevailing rates.

11.8 Whilst the law that governs this Agreement is set out and in clause 17 of the General Terms and Conditions, the Client acknowledges that the Hosted Services, for which the Company acts solely as an agent for the Client, are provided under Microsoft's terms and conditions which are governed by Applicable Law.

Service Schedule

1. Services Summary

1.1 The Company procures subscriptions to a number of Microsoft 365 packages and Azure as set out on the Order.

1.2 The Company provides IT Support Services as set out in paragraphs 3 to 6 of this Service Schedule.

2. Support Tiers

Support Tiers, which are set out on the Order, are provided dependent on the Microsoft 365 licence type Subscription as follows:

- Tier 1 requires a Microsoft 365 Business Premium Licence
- Tier 2 requires a Microsoft 365 E3 Licence
- Tier 3 requires a Microsoft 365 E5 Licence

3. Services provided under all support tiers

3.1 Service Desk

3.1.1 Subject to fair use, the Company's Service Desk provides support and assistance in the use of the IT Equipment, including the following:

- Management of the prompt resolution of Incidents arising within the IT Equipment which are raised by the Client
- Management of the prompt resolution of Incidents arising within the IT Equipment which are identified by the Company's monitoring system
- Escalation management if required in the event of protracted Incident resolution
- Management of change requests
- Remote access support if possible and appropriate

3.1.2 The Client shall report Incidents by one of the following methods:

- By Email to the Company's Service Desk: servicedesk@pstg.co.uk
- By Telephone to the Company's Service Desk: 0203 907 9570

3.1.3 The Service Desk is available during the Hours of Cover, which are from 8am to 6pm Monday to Friday, excluding bank and public holidays.

3.1.4 The Company's Service Desk response and resolution targets are:

Priority Level	Reporting Method	Target Response Time	Target Resolution Time
1	Telephone	Immediate	Two Working Hours
2	Telephone	Immediate	Four Working Hours
3	Telephone or email	Eight Working Hours	One Working Day
4	Telephone or email	Eight Working Hours	Three Working Days
5	Telephone or email	Eight Working Hours	Five Working Days

3.1.5 The Company will use reasonable endeavours to provide a fix or work-around within the target timescales set out in sub-clause 3.1.4

3.1.6 Incident priority levels are defined as:

Priority Level	Description
1	Business-critical system failure
2	VIP or service affecting with more than one End User affected
3	Single End User affected
4	Non-urgent, peripheral not working
5	Service Request for configuration change that does not require change management

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

- Name of Client and person raising the Ticket
- Contact telephone number
- Description of the Incident
- Description of actions taken prior to the Incident occurring
- Explanation of how the Incident has been diagnosed
- Any other relevant information

3.1.8 The Company shall make reasonable endeavours to meet the targets set out in this paragraph 3. Failure by the Company to meet such targets shall not be deemed a breach of this Agreement.

3.2 Backup Service for Microsoft 365

The Company's Backup Service for Microsoft 365 protects the Client against loss of data that is held within Microsoft's cloud infrastructure. Unexpected data loss can typically be due to user error or occur if an End User subscription expires, and the Company's service, in addition to providing the Client with additional control over its data, mitigates the risk of such data loss.

3.2.1 The Company will back-up the Client's Microsoft 365 data based on the number of End Users and storage capacity set out on the Order; backup data is stored on a backup appliance which is located at the Company's Data Centre.

3.2.2 Microsoft 365 backups include:

- OneDrive file and folder data backups (documents), per End User
- Exchange data, including emails, email attachments, notes, deleted items, contacts (excluding photographs), tasks and calendar events (including attendees, recurrence, attachments and notes)
- SharePoint primary, custom, group and team site collections; folders, document libraries and sets; site assets, templates and pages
- Groups (including conversations, plans, files, sites and calendar)
- Teams (including wiki and chat)
- Audit logs, data controls and export capabilities

3.2.3 Backups can be configured to run automatically or on-demand.

3.2.4 The Backup and Recovery Service is fully managed by the Company.

3.2.5 The backup system will automatically notify the Company of backup success or failure.

3.2.6 Backups are encrypted at rest and during transmission.

3.2.7 Backup data will be retained for ninety days.

3.2.8 Data restoration:

- Data restores will only be initiated by the Company when requested by an authorised representative of the Client
- The Company will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Client
- The Company will use reasonable endeavours to restore data to the location that is specified by the Client

3.2.9 Whilst the Company shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, the Company will carry out the following activities during the Working Day:

- Respond to Client requests for data restores
- Respond to and investigate any Incidents that arise in the service which cannot be remediated automatically, whether raised by the Client or by the Company's Monitoring Agent

3.2.10 Quarterly Data Restore

The Company will perform quarterly test restores of backed-up data to ensure that backups are functioning correctly. This will be implemented by the Company contacting the Client to agree a test target (for example a mailbox or SharePoint Site) and carrying out the test restore at an agreed time. The results from the test will be presented at the quarterly review meeting.

3.3 Enhanced Email Protection

Enhanced Email Protection is provided by Exchange Online Protection, which provides:

- Elimination of threats before they reach the corporate firewall by using multi-layered, real-time anti-spam and multi-engine anti-malware systems
- Active content, connection, and policy-based filtering that enable compliance with corporate policies and government regulations
- Protection for the Client's IP reputation by using separate outbound delivery pools for high-risk email
- Near real-time reporting and message trace capabilities providing insight into email environments by retrieving the status of any message that Exchange Online Protection processes

The Company will ensure that the Client's Enhanced Email Protection is installed, correctly configured, up to date and is correctly functioning.

3.4 Auditing and Reporting

The Company will provide support and guidance on the use of product auditing and reporting tools and will provide monthly reports which include:

- Service metrics (Incidents raised, resolved, resolution performance against SLA)
- Users and active system accounts
- Supported Hardware
- Installed supported software
- Hosted Service performance / availability
- Patch update status

3.5 User Management

The Company will ensure that Microsoft Windows and Microsoft 365 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 or remove email accounts, data folders and shares, and the related security permissions
- De-provisioning and re-provisioning existing Endpoints and other devices

3.6 Office365 Tenant Management

The Company will provide management of the Microsoft 365 tenant, including addition of DNS records.

3.7 SharePoint Management

In response to Service Requests, the Company will assist with the creation (but not configuration) of new SharePoint Sites and Libraries.

3.8 Third-Party Issue Management

The Company 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.

3.9 Endpoint Protection

Endpoint Protection, which provides:

- Endpoint protection using a unified endpoint platform for preventative protection, post-breach detection, automated investigation and response
- Safeguarding against malicious threats posed by email messages, links (URLs) and collaboration tools

The Company will ensure that the Client's Endpoint Protection software is installed, correctly configured, up to date and is correctly functioning.

3.10 Office365 Application Support

Office 365 Application Support includes support for the configuration of the following products (as set out on the Order):

- Email and Calendar
- OneDrive for Business
- Voicemail integration with Exchange (where the Company manages all components of voicemail and Exchange services)
- Support for the following products is limited to resolving service availability issues:
    - Teams
    - SharePoint
    - Yammer
    - Office Online Applications
    - Planner
    - Sway
    - Delve

- Rights Management Services

4. Services provided under tier 1 only

4.1 IT Surgery 1

An engineer from the Company will visit the Client's Site for one day once a month. During the visit, the engineer will be available to provide usability training for Microsoft 365 applications (up to a maximum group size of ten people) and to assist in the remediation of any outstanding Incidents.

5. Additional Services provided under tiers 2 and 3

5.1 Advanced Office 365 Email and Data Protection

Enhanced Email Protection is provided by Exchange Online Protection, which provides:

- Elimination of threats before they reach the corporate firewall by using multi-layered, real-time anti-spam and multi-engine anti-malware systems
- Active content, connection, and policy-based filtering that enable compliance with corporate policies and government regulations
- Protection for the Client's IP reputation by using separate outbound delivery pools for high-risk email
- Near real-time reporting and message trace capabilities providing insight into email environments by retrieving the status of any message that Exchange Online Protection processes

Endpoint and cloud anti-virus, which provides:

- Endpoint protection using a unified endpoint platform for preventative protection, post-breach detection, automated investigation and response
- Safeguarding against malicious threats posed by email messages, links (URLs) and collaboration tools
- Identity protection using Active Directory Domain Services signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions
- Protection for cloud-based applications using a comprehensive cross-SaaS solution which delivers deep visibility, strong data controls and enhanced threat protection

The Company will ensure that the Client's Enhanced Email Protection and Endpoint anti-virus software is installed, correctly configured, up to date and is correctly functioning.

5.2 Mobile Device Management

Mobile device operating system security and management is provided to devices that are enrolled with Microsoft InTune. 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.

5.3 Windows 10 Management

Management and support of application deployment and security policies applied to the Client's corporate owned Windows 10 based Endpoints.

5.4 IT Surgery 2

An engineer from the Company will visit the Client's Site for one day twice a month. During the visit, the engineer will be available to provide usability training for Microsoft 365 applications (up to a maximum group size of ten people) and to assist in the remediation of any outstanding Incidents.

5.5 Centralised Updates and Patching

Install white-listed patches as they are made available for the Windows 10 Software that is listed on the Order.

5.6 Advanced Monitoring and Resolution

The Company will monitor key performance aspects of hosted Microsoft 365 and Azure Software 24 x 7 x 365 and automatically resolve Incidents or potential Incidents whenever possible. The Company shall respond to any Incidents that cannot be automatically resolved during the Hours of Cover in a manner that is appropriate to the severity of the Incident, whilst aiming to minimise disruption to the availability of the hosted Software. The Company shall also:

- Monitor and schedule Microsoft 365 tenant updates
- Review and if appropriate respond to best practice guidelines announced by Microsoft
- Advise the Client on relevant industry changes

5.7 Strategic Roadmap

The Company will provide input into the Client's strategic roadmap:

- Understand the Client's business requirements to determine recommendations and changes where appropriate
- Offer advice on current landscape and technology changes
- Offer input to future strategy and budgeting

6. Additional Services provided under tier 3 only

6.1 Accessory Support

The Company will Triage Incident that occur with keyboards, mice and printers and provide diagnostic information which may be used either to resolve the Incident or if resolution is not possible, provide advice on options for replacement.

6.2 VIP Support

Service Desk Hours of Cover will be extended to 24 x 7 x 365 for named End Users.

6.3 Reserve Equipment

The Company will hold in stock Reserve Equipment as set out on the Order. The Client may call off such Reserve Equipment at any time, either as a replacement for faulty IT Equipment or for use by new employees.

6.4 Call Out and 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 Working Day
- Subject to fair usage, 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

7. Complaint Handling

7.1 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 Desk Engineer	0203 907 9570
2	Service Desk Team Leader	0203 907 9567
3	Cloud Services Director	0203 907 9481

7.2 Formal complaints can be made by e-mail or telephone, and will be responded to within three Working Days.