Supplementary terms for the supply of Network and System 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 'Cloud-Based Utilities' means the collection of ancillary third-party provided services, including backup, anti-Malware, and Monitoring Services which will be used by the Company in support of the Network and System Support 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 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.

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

1.6 '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.

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

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

1.9 'IT Equipment' means servers and Endpoints installed at the Client's Site, which is listed in the System Documentation and is to be supported under the terms of this Agreement.

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

1.11 'Hosted Services' means cloud-based Microsoft 365 and Azure services as provided by the Company under the terms of a Subscription Services Agreement.

1.12 'Line of Business Application' means third-party software which provides solutions to specific Client business requirements.

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

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

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

1.16 'Network Equipment' means the the equipment that underpins the Local Area Network.

1.17 'Monitoring Services' means the Company's monitoring services that remotely monitor the performance of IT Equipment and Hosted Services.

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

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

1.20 'Server' means an item of IT Equipment provides centralised resources, data and services to other IT Equipment in the Local Area Network.

1.21 'Services' means Network and System Support Services.

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

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

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

1.25 'Software' means the software which is installed on and is a component of the Hosted Services or IT Equipment, as listed in the System Documentation.

1.26 'System Documentation' means the documentation to be provided by the Company which describes each component of the IT Equipment and Hosted Services that are to be supported under the terms of this Agreement.

1.27 '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 the same as the Minimum Term, unless otherwise agreed. 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 Network and System Support Services are provided to support the Client's on-premise IT systems and Hosted Services. Network and System Support Services will be provided by the Company both remotely and at the Client's Site. For the avoidance of doubt, Network and System Support Services do not include the provision or support of network connectivity outside of the Client's Site.

3.2 The Network and System Support Services to be provided hereunder shall include those set out in the Order and described in the Service Schedule.

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

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

3.5 The Company provides Cloud-Based Utilities under the terms of this Agreement; and:

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

3.5.2 The Company cannot guarantee and does not warrant that the Cloud-Based Utilities will be free from interruptions, including:

a) Interruption of the Cloud-Based Utilities for operational reasons and temporary degradation of the quality of the Monitoring Services;

b) Interruption of the network connection between the Cloud-Based Utilities and the IT Equipment; and

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

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

3.6 Network and System Support Services are provided to support the Hosted Services and the IT Equipment. For the avoidance of doubt, Network and System 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.

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 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

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

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

5.3 Use reasonable endeavours to ensure that user-names, passwords and personal identification numbers are kept secure and:

5.3.1 In line with current best practice, change access passwords for all equipment that in the Client's reasonable opinion, may be liable to access by unauthorised persons;

5.3.2 Change passwords as appropriate when employees leave;

5.3.3 Use strong passwords;

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

5.3.5 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.

5.4 Be responsible for the authorisation of changes proposed by the Company to the configuration of the Local Area Network.

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

5.6 Accept that if it attaches equipment that does not comply with the provisions of sub-clause 5.5 ('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:

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

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

5.6.3 Request that the Client disconnect the Unauthorised Equipment from the IT Equipment or Hosted Services; and if such request is not agreed by the Client within thirty days, terminate this Agreement forthwith.

5.7 Accept that is the Client's sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training to prevent the introduction of Malware into the IT Equipment or Hosted Services.

5.8 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.

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

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

5.11 Provide the Company with global administrator access permissions.

5.12 During term of this Agreement maintain a level of cyber-breach insurance cover that is appropriate to the risks associated with accidental destruction, damage, loss or disclosure of Client Data; general insurance to cover loss of or damage to the IT Equipment; and

5.12.1 In response to reasonable requests made by the Company, provide evidence to show compliance with this sub-clause;

5.12.2 Not do or omit to do anything which would destroy or impair the legal validity of the insurance;

5.12.3 If the Client suffers a Data Security Event and subsequently requests assistance from the Company, ensure that such request for assistance will not breach the terms of the insurance policy prior to requesting assistance from the Company;

5.12.4 Acknowledge that insurance will not relieve the Client of any liabilities under this Agreement.

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.

6.2 During the Hours of Cover set out in the Service Schedule, make available a Service Desk that shall provide support and guidance in the use of the IT Equipment and / or Hosted Services and manage the resolution of all Incidents raised by the Client.

6.3 During the Hours of Cover set out in the Service Schedule, make available a Site-based engineer ('Engineer') who shall carry out a number of the Service Components and assist in the resolution of Incidents raised by the Client; however

6.3.1 During times of the Engineer's leave of absence, support will be provided by the Company remotely.

6.4 Prior to commencement of the Services, install its Monitoring Agents on the Client's Servers.

6.5 Provide Monitoring Services 24 x 7 x 365 and respond to any alerts raised by the Monitoring Services during the Hours of Cover set out in the Service Schedule.

6.6 Respond to Tickets raised by the Client and make reasonable endeavours to resolve any Incident that occurs within the IT Equipment or Hosted Services.

6.7 Proactively respond to Tickets raised by the Monitoring Agents and make reasonable endeavours to resolve any Incident that occurs within the IT Equipment or Hosted Services.

6.8 Maintain the System Documentation.

7. Clause Intentionally Unused

8. GENERAL

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

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

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

8.2.2 Terminate this Agreement.

8.3 The Company may perform any Planned Maintenance that may limit the availability of the Cloud-Based Utilities. Planned Maintenance will be scheduled to minimise disruption to the Client. The Client will be notified at least forty eight hours prior to such Planned Maintenance taking place.

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

8.5 If the Client suffers a Data Security Event and subsequently requests assistance from the Company, it is the Client's sole responsibility to ensure that such request for assistance will not breach the terms of any cyber-insurance policy that the Client has in place, prior to requesting assistance from the Company.

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, costs, losses or damages incurred by the Client 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 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.

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 Company at any time if it can no longer provide the Services;

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

9.1.4 By the Client if the Company or its supplier makes changes to the Network and System Support 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 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 Network and System 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.

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

10.7.1 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;

10.7.2 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.

10.8 The Client shall not be liable for termination Charges if this Agreement is terminated:

10.8.1 By 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;

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

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

11.5 Patches are supplied by Company-approved software vendors and not the Company. The Company will use reasonable endeavours to prevent a patch causing an adverse reaction with any particular machine configuration, but the Company shall not be liable for any disruption resulting from the

installation of patches. In such circumstances, the Company's sole responsibility will be to de-install the patch or roll back to an appropriate restore point to resolve the Incident.

11.6 The Services provided by the Company under the terms of this Agreement are solely Network and System Support Services and do not include:

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

11.6.2 The investigation of the causes of Data Security Events.

11.7 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.

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

11.9 This Agreement does not include:

11.9.1 The support of any equipment that is not listed in the System Documentation;

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

11.9.3 The supply of any consumables;

11.9.4 Recovery of Client data whose loss can be reasonably attributed to accidental deletion, mis-use or negligence by the Client, where such recovery necessitates work other than recovery from the latest backup or the number of requests for such is in the Company's reasonable opinion, excessive;

11.9.5 The recovery of Client's data that results from Malware infection where such recovery necessitates work other than recovery from the latest backup or the number of requests for such is in the Company's reasonable opinion, excessive;

11.9.6 Remediation following a cyber-breach or hack where either the Client has previously failed to act on recommendations made in relation thereto by the Company or the number of requests for such is in the Company's reasonable opinion, excessive;

11.9.7 Remediation of Incidents caused by Windows 10 or 11 feature upgrades where the Client has failed to follow recommendations made in relation thereto by the Company;

11.9.8 Operating system installation or re-installation where the Client has failed to follow recommendations made in relation thereto by the Company;

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

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

11.9.11 The installation of Software;

11.9.12 Support for any Software that is not supported by its manufacturer or Line of Business Applications;

11.9.13 The provision of development projects;

11.9.14 The provision of End User or "how to" training, unless otherwise agreed and subject to Fair Use;

11.9.15 Support for internet service provider outages;

The Company may at its sole discretion provide any of the excluded services listed in this sub-clause 11.9, and charge for the supply thereof at its prevailing rates.

Service Schedule

1. Service Desk

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

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

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.

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

1.5 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

1.6 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

1.7 The Company shall make reasonable endeavours to meet the targets set out in this paragraph 1. Failure by the Company to meet such targets shall not be deemed a breach of this Agreement.

2. On-Site Support

Subject to customary leave of absence (during which time support will be provided remotely), the Company will provide an on-site Engineer during the Hours of Cover. The maximum duration of any one period without On-Site Support will be limited to fourteen days. On receipt of a Ticket, the Service Desk will either attempt to resolve the Incident remotely or at its discretion pass the Ticket to the Engineer for resolution. To ensure that Tickets are properly recorded and resourcing conflicts are properly handled, the Client should report all Tickets via the Service Desk rather than making direct requests to the Engineer. If direct requests are made to the Engineer, the Engineer will direct the Client to the Service Desk. The Engineer shall be responsible for Incident resolution activities and either providing or providing input into the execution of the Service Components listed in paragraphs 3 to 18 below.

3. 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

4. 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

5. System Documentation Maintenance

The Company maintain the System Documentation and ensure that it accurately reflects the IT Equipment, Hosted Services and network infrastructure (including all additions, changes and deletions) that is supported under the terms of this Agreement.

6. 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

7. Office365 Tenant Management

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

8. SharePoint Management

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

9. Third-Party Incident 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 Incidents with the third-party software or services.

10. Office365 Application Support

Office 365 Application Support includes support for the configuration of the following products (as set out in the System Documentation):

- 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 Incidents:
  - Teams
  - SharePoint
  - Yammer
  - Office Online Applications
  - Planner
  - Sway
  - Delve
  - Rights Management Services

11. Windows Management

Management and support of application deployment and security policies applied to the Client's corporate owned Windows 10 and 11 based Endpoints.

12. Centralised Updates and Patching

Install white-listed patches as they are made available for the Windows 10 and Software that is listed in the System Documentation.

13. 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

14. 24 x 7 Network Monitoring

14.1 The Company's network monitoring service is a powerful platform for managing Network Equipment for ensuring optimal network performance and reducing the risk of service impact due to network related issues. The Company will provide the following services:

SNMP network monitoring
Trouble-shooting, fault diagnosis and remediation
Network documentation
IP address management
Alerts and notifications
Service monitoring
Usage and health statistics
Live and historic data
Configuration management
Configuration restore
Configuration analysis

14.2 Network topology maps are automatically generated and maintained along with device configuration backup and configuration change notification and comparison.

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

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

14.5 The Company's Monitoring Agent will scan for managed Network Equipment which will automatically be added to the service. This includes managed switches, routers, firewalls, wireless access controllers and wireless access points. Unmanaged devices will not be added to the service and will not be charged.

14.6 Hardware maintenance / manufacturer's warranty is required to be in place on all Network Equipment that is covered by the Company's advanced network monitoring service.

14.7 The Company's network monitoring service does not include:

- Identifying every device discovered on the network
- Configuring Windows Management Instrumentation
- Wireless security scans for rogue access points or other issues
- Network reconfiguration

15. Managed Firewall Service

The Company's Managed Firewall Service includes two services, Firewall Management and Firewall Content Management.

15.1 The Firewall Management Service includes:

- Updating firmware and software to maintain security levels
- Managing access in response to Client requests

- Changes to rules in response to Client requests

15.2 Firewall Content Management

The Firewall Content Management service provides filtering of access to websites, allowing the Client to selectively block End User access to specified websites. The service includes:

- Set up and configuration of Firewall Content Management service
- Changes to setup, including unblocking websites, making exceptions for users and individual Endpoints in response to Client requests
- Checking blockages and resolving content filtering issues

16. Wireless LAN

To ensure the secure, optimum-performance operation of the Client's Wireless LAN, the Company provides the following services:

- Basic network monitoring, including router/web and wireless access point connections
- Trouble-shooting and performance / fault diagnosis and remediation
- Updates to Network Equipment configurations, including performance optimisation and in response to best practice
- Firmware and security updates and their installation
- Guest access control

17. 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.

18. Line of Business Application Support

The Company will pass on details of issues to third-party suppliers of Line of Business Applications that are listed in the System Documentation and manage the resolution of such issues.

19. Complaint Handling

19.1 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	Email Address
1	Service Desk Engineer	0203 907 9570	support@pstg.co.uk
2	Service Desk Team Leader	0203 907 9567	support@pstg.co.uk
3	Cloud Services Director	0203 907 9481	bward@pstg.co.uk

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