Supplementary terms for the supply of Managed Backup 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 'Managed Backup Services' means services that provide data backup for Servers and Microsoft 365 accounts.

1.2 'Cloud-Based Utilities' means the ancillary third party- provided services, including backup and backup monitoring which will be used by the Company in support of the Managed Backup Services.

1.3 'Configuration' means the configuration of the backup.

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

1.5 '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.

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

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

1.9 'IT Equipment' means Servers, virtual Servers and Workstations.

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

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

1.12 'Scoping Document' means the document that if set out on the Order, will be provided by the Company and describes the scope of the Services to be provided.

1.13 'Server' means IT Equipment which functions as a server, including physical and virtual servers.

1.14 'Service Desk' means the Company's dedicated team of qualified support technicians.

1.15 'Service Request' means a requirement for a change to the configuration of the Managed Backup Services.

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

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

1.18 'Workstation' means IT Equipment which functions as a desktop workstation or laptop computer.

2. TERM

2.1 This Agreement will be deemed to come into effect on acceptance of the 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 Managed Backup Services are provided to enhance the security of the Client's data. Managed Backup Services will be provided by the Company remotely. For the avoidance of doubt, Managed Backup Services do not include the provision or support of network connectivity outside of the Client's Site, which is required to enable the Services.

3.2 The Services comprise Managed Backup Services which are described in the Service Schedule. The Company shall use reasonable endeavours to provide the Managed Backup Services 24 x 7 x 365. The Services include:

3.2.1 Server Backup; and / or

3.2.2 Microsoft 365 account backup;

as set out on the Order.

3.3 Certain Managed Backup Services provided by the Company rely upon Cloud-Based Utilities and:

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

3.3.2 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 Cloud-Based Utilities;

b) Interruption of the connection of the Cloud-Based Utilities to other network services provided either by the Company 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.

3.3.3 Although the Company 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 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.

3.4 If set out on the Order, the Company will create a Scoping Document and the Services described in the Service Schedule will be provided in accordance with the Scoping Document.

4. ACCEPTABE USE

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

4.2 The Client agrees to ensure that the Services is not used by its End Users to:

4.2.1 Store materials or data breach of the rights of third parties, including but not limited to those of quiet enjoyment, privacy and copyright;

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

4.2.3 In any manner which in the Company's reasonable opinion brings the Company's name into disrepute;

4.2.4 Act in any way which threatens the security or integrity of the Managed Backup Services.

4.2.5 Connect to the Managed Backup Services insecure equipment or services able to be exploited by others to carry out actions which constitute a breach of this Agreement.

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

4.4 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 Ensure that user-names, passwords and personal identification numbers are kept secure and:

5.3.1 On a regular basis, change access passwords for all IT Equipment that in the Client's reasonable opinion may be liable to access by unauthorised persons.

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, to prevent the introduction of Malware into the IT Equipment.

5.5 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 the Company.

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 Managed Backup Services set out in the Order and described in the 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 Services and manage the resolution of all Managed Backup Services-related Incidents raised by the Client.

6.3 Monitor the performance of the Managed Backup Services.

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

6.5 Proactively respond to Incidents reported by the Managed Backup Services and make reasonable endeavours to repair any Incident that is within the services.

7. Clause Intentionally Unused

8. GENERAL

8.1 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.

8.2 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 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.

8.5 The Client hereby consents to the Company and its sub-contractors accessing Servers and Workstations that are backed up under the terms of this Agreement, 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 at 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.

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, including any set-up and installation Charges will be raised in arrears.

10.3 The Company shall commence charging for the Managed Backup Services from the RFS Date, regardless of the date on which the Client commences use of the Managed Backup 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 The Client agrees that it shall be liable for termination Charges if this Agreement is terminated by:

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

10.5.2 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.

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

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

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

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

10.6.4 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;

10.6.5 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 of the Service is intended to proactively identify most system-related issues, the Company does not warrant and cannot guarantee that the its monitoring will identify all Service-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 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.

11.4 This Agreement does not include:

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

11.4.2 The recovery of Client's data that results from Malware infection.

The Company may at its sole discretion provide any of the excluded services listed in this sub-clause 11.4, and charge for the supply thereof at its prevailing rates.

Service Schedule

Under the terms of this Agreement, the Company will provide Server Backup and Recovery, Microsoft 365 Backup and Recovery or both, as set out on the Order.

1. Server Backup and Recovery

1.1 The Company provides a number of backup and recovery options. The options selected are set out on the Order. Options include:

- Backup to a resilient backup appliance which is located at the Client's Site
- Backup to a resilient backup appliance which is located at the Client's Site, an image of which is backed up in the Company's Data Centre
- Backup to a resilient backup appliance which is located at the Client's Site with a parallel backup to the Company's EU-based Data Centre
- Cloud-based backup with backup data held at either the Company's Data Centre or at a location specified and under the responsibility of, the Client
- Cloud-based Data retention with retained data held at either the Company's Data Centre or at a location specified and under the responsibility of, the Client
- Dependent on the options selected, backups can be made at image (Server or virtual Server) or file / folder level

1.2 The Company's Data Centre is EU-based.

1.3 Backups are encrypted at rest and during transmission.

1.4 The Backup and Recovery Service is fully managed by the Company and if set out on the Order will be managed in accordance with the Scoping Document.

1.5 The backup system will automatically notify the Company of backup success, errors and failures;

1.6 In the event of a backup failure, the Company's support team will receive an alert from the backup system and will investigate the problem to identify the root cause.

1.7 Backup frequency and retention periods are set out on the Order.

1.8 Data restores are only initiated when requested by an authorised Client representative; and

- The recovery point objective will be no later than the time of the backup prior to the system failure that resulted in the request for restoration
- The recovery time objective will be determined by the Hours of Cover
- Data can be restored at various levels of granularity, including image, folder or file level, as requested by the Client

1.9 Disaster Recovery

1.9.1 Some of the backup and recovery options offered by the Company include facilities to manually (that is, the recovery mode is active-passive) spin up a disaster recovery server in the event a 'disaster' at the Client's Site. Dependent on the options selected, the disaster recovery server may be located:

- On the Client's Site-based resilient backup appliance
- At the Company's Data Centre, where such service will be available for a number of days, as set out on the Order

1.9.2 If the Client's server becomes unavailable for use, the Company will either:

- Initiate failover to the backup appliance at the Client's Site; or

- Initiate failover to a disaster recovery server within its Data Centre and provide temporary access to the Client's End Users until such time as access to the server is restored

1.10 The recovery point objective will be determined by the backup and recovery option selected.

1.11 The recovery time objective will be determined by the Hours of Cover.

1.12 If requested, the Company shall carry out disaster recovery testing as agreed with the Client; such testing will be chargeable at the Company's prevailing rate.

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.

2.1 The Company will retain 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.

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 for 365 days

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

2.4 The Backup and Recovery Service is fully managed by the Company and if set out on the Order will be managed in accordance with the Scoping Document.

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

2.6 Backups are encrypted at rest and during transmission.

2.7 Backup data will be retained for ninety days.

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

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 Hours of Cover:

- 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 agents

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. Service Request Processing

Service Requests shall be limited to changes to the backup Configuration of the existing Services and subject to fair use shall not result in changes to the Charges made for the Services. Backups for additional End Users or Servers will be subject to a new Order.

3.1 The Company shall process a Service Request made by the Client as follows:

- The Company shall verify the Service Request and notify the Client of its response
- Provided that the Company agrees with the Service Request, the Company shall implement the change
- If the Company does not agree with the Service Request, the Company will explain the reasons, including any associated risks, to the Client ('Queried Service Request')

3.2 The Client may formally (ie, in writing) request that the Company implement a Queried Service Request. In response to such a request, the Company may at its sole discretion, do either:

- Implement the Queried Service Request on the understanding that the Client understands and accepts the risks involved. Under these circumstances the Company shall have no liability to the Client in the event that the change causes degradation to the Service, including malfunctioning or security risk
- Offer to provide consultancy services to the Client, with the objective of finding an alternative solution. Consultancy is chargeable at the Company's prevailing rate

3.3 The Company will normally implement agreed Service Requests during the Working Day. If requested, the Company may implement Service Requests outside of the Working Day, and will be entitled to charge the Client at its prevailing rate.

4. Service Desk

4.1 During the Working Day, the Company's Service Desk provides support and assistance in the use of the Managed Backup Services, including the following:

- Management of the prompt resolution of Incidents arising within the Managed Backup Services which are identified by the Company's monitoring system
- Management of the prompt resolution of Incidents arising within the Managed Backup Services which are raised by the Client
- Escalation management if required in the event of protracted issue resolution
- Management of Service Requests made by the Client
- Monitoring the Backup Service for availability

4.2 The Client shall raise Incident reports 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
- Via the Company's support portal: pstg.myportallogin.co.uk

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

4.4 The Company shall aim to make an initial response to the Client's request for assistance within one Working Day of the Client raising the Ticket report and shall use reasonable endeavours to resolve the Incident within five Working Days.

5. Complaint Handling

5.1 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	Head of Delivery	0203 907 9561

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