

1. Service Overview

Our Cloud Back-up Service provides back-up features such as file-level, disk-level application backups. Our Cloud Back-up Service provides back-up features such as file-level and M365 backups.

This Service is offered as a Managed Backup Service or Self-managed Service:

- (a) If you procured the Managed Backup Service, Six Degrees will manage
 - (i) Reschedule or reconfigure backups
 - (ii) Suspend backups
 - (iii) Delete or remove backups
 - (iv) Configure new backups
 - (v) Restore from backups
 - (vi) Set-up or change backup configuration

we would also utilise a centralized web dashboard to provide reporting and monitoring.
- (b) If you procure the Self-Managed Service, you will retain management responsibilities and self-serve your configuration, scheduling, retention, monitoring, reporting and encryption setup. Should you choose this model, you will be responsible for all activities related to management and recovery of your backups.

Your data will automatically be subject to de-duplication and compression, regardless of whether you are procuring our Self-Managed or Managed Backup Service. Depending on your data, this deduplication can achieve a ratio of up to 10:1 reduction.

All your backup data will be encrypted in transit and at rest using Advanced Encryption Standard ("AES") with 128, 192, or 256-bit keys, with 256 being the default. This AES requires a user-defined password that we will store for managed customers and employs end-to-end encryption to secure data at the source before transmission and during storage. Please note that if you are procuring our Self-Managed Service, it will be your responsibility to create and safely store your AES password.

As a standard, all backed up data will be stored in a single UK data centre with internal redundancy. Any different region that we may agree with you will be documented in your Statement of Work (SoW).

Details of your Service will be included in your Order Form and/or SoW, including your choice of Managed Backup Service or Self-Managed Service and the associated Fees.



Our Cloud Back-up Service can be procured as a standalone or in conjunction with our Public or Private Cloud Service offering. Please see the relevant Service Description for further details.

2. Service Features

2.1 Cloud Backup Service

Our cloud backup platform includes the features listed in the table below. Please note that these features will be available for both the Managed Backup Service and Self-Managed Service.

Features	Description
File-level, disk-level and application backups.	The backup platform allows for backup and restoration of individual files, applications and folders.
Additional Backup workloads	This Service supports a range of workloads, including Mac, Windows, Linux and Microsoft 365
Local UK / International storage options	By default, data will be secured in UK-based cloud storage locations; however, international storage options may be available if required. Please contact us if you wish to discuss your options.
Flexible recovery options	The backup platform provides flexible recovery options, allowing you to restore to granular files.
Adjustable backup frequency for Microsoft 365	The backup platform offers options for automated daily backups, multiple daily backups, on-demand backups, and automatic new user detection.
Archive/ backup encryption	Encrypts backups using AES with 128-bit, 192-bit, or 256-bit keys, ensuring data security and compliance.
Incremental and differential backups	The backup platform allows you to adjust the frequency and type of your backups.
Immutable backups	Allows users to prevent data from being altered or deleted to mitigate the risk data loss due to accidental or malicious actions.
Deduplication	The backup platform automatically eliminates duplicate copies of repeating data to reduce storage requirements.
Standard monitoring and reporting	You will be able to view standard monitoring activities and reports on your backup service.
Group management for Microsoft 365	The backup platform will allow you to assign policies and tasks to multiple users within your Microsoft 365 environment.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

4. Service Implementation of Cloud Back-up	Us	You
Self-Managed Backup Service		
We will send you a welcome pack.	•	
We will run internal acceptance tests to confirm your environment is ready.	•	
We will facilitate a training call on using the backup software and admin portal.	•	



4. Service Implementation of Cloud Back-up	Us	You
We will confirm the Ready for Service Date, send you the handover pack and commence billing for your Service.	•	
You will install the relevant agents, backup schedules and retention periods.		•
Managed Backup Service		
We will install the relevant agents, backup schedules and retention periods	•	
We will configure the backup schedule and retention for all Protected Servers.	•	
We will undertake initial backup and testing for all the Protected Servers.	•	
We will perform the acceptance test (including restore activity) and notify you of any issues that we identify (this process may involve your third party vendors).	•	
We will perform initial backup and confirm completion to you, then move to steady state incremental backups.	•	
We will confirm the Ready for Service Date, send you the handover pack and commence billing for your Service.	•	

4.1 Delivery phases

We will agree with you the details of the implementation process and the associated key milestones based on your requirements and document this process in your SoW.

3.2 Ready for service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the implementation steps and testing are complete and that the Service is ready for service. This date may be specified to occur at a later date, if mutually agreed to be so. If you consider that the Service is not ready for service on the date notified, you must notify us within two (2) weeks of our notification, after which the Ready for Service date will be deemed to have occurred regardless of issues or defects of which you may later become aware and notify us about (which will then be dealt with as faults or service issues but will not change the Ready for Service Date).

5. Billing

The Service will be billed as a Recurring Fee and Usage Fee from the Ready for Service Date as specified in your Order Form. There will also be a Non-Recurring Fee for each of the service implementation phases.

5.1 Pricing Models

(a) Per Workload model

This is the pricing model that we offer as a standard.

We will charge you a fixed Recurring Fee per Workload, and stored data in GB as specified in your Order.



Within this model, you commit to a monthly quota of storage for your backup data. If the quantity of backed up data exceeds your monthly storage commit, then any additional storage may not be backed up.

You will be notified when you are approaching, and reach your quota, and can increase your commit when necessary.

(b) Microsoft 365 per Seat Model

If you are procuring this Service to back up your Microsoft 365 environments, you can select this optional pricing model to pay a fixed Recurring Fee for each of your Microsoft seats (users).

(c) Per GB Model

We will charge you a fixed Recurring Fee for a specific GB monthly allowance (as specified in your Order Form).

Within this model, you commit to a monthly quota of storage for your backup data. If the quantity of backed up data exceeds your monthly storage commit, then any additional storage may not be backed up.

You will be notified when you are approaching, and reach your quota, and can increase your commit when necessary.

5.2 Additional Charges

We reserve the right to charge additional fees in the following situations:

- (a) Any service request in excess of the monthly allowance set out in Section 6 below;
- (b) Any change in your requirements occurring after the implementation of the Service and/or outside the scope of this Service Description, which we will charge as a professional services engagement; and
- (c) Any training that you require beyond the initial training courses that we provide as part of the Service implementation activities described at Section 3, which we will charge as a professional services engagement.

6. Service Operations

Please refer to the Operations Manual for information on incident management, requests for change and for information.

If you are procuring the Self-Managed Service, we will include information on our incident management process in your Welcome Pack.

Service Request Entitlement

A service request for this Service is defined as one (1) request of the following items:

Service Request	Self-Managed Service	Managed Backup Service
-----------------	----------------------	------------------------



Reschedule or reconfigure backup		•
Suspend backup		•
Delete or remove backup		•
Configure new backup		•
Restore from backup		•
Set-up or change backup configuration		•
Portal account administration	•	•
Service availability faults	•	•

As standard, for managed customers we offer 5 services requests per month, with up to 5 changes within each service request permitted. This begins after signoff of initial configuration.

We can implement additional service requests as and when required for an additional Fee which will be defined in your Order Form or SoW. Although we may accept multiple requests on a single support ticket for administrative convenience, we will count each change requested on the same ticket as an individual service request.

We will implement standard service requests listed in the table above in accordance with the resolution times set out in Section 12 but, in any case, in no less that forty-eight (48) hours from receipt of the request. Please ensure to submit any urgent change, amendment or cancellation request at least forty-eight (48) hours prior the desired implementation date.

7. Termination

Upon termination of your Cloud Back-up Service, you have three options regarding your data:

- (a) **Data deletion by default:** By default and unless otherwise agreed with you, we will delete your data upon termination of your Cloud Back-up Service, and ensure that no residual data remains on our servers. We will notify you prior to the deletion to give you the opportunity to secure your data before it is permanently removed.
- (b) **Transfer to another provider:** Alternatively, you can engage with your replacement partner provider for the transfer and setup of your tenant . If you choose this option, we will use reasonable efforts to facilitate the transfer of your tenant, however you will remain responsible to coordinate with your replacement provider.
- (c) **Bespoke professional services engagement:** If you wish to keep and restore some of your existing data, we can provide additional professional services (PS) to assist you with these activities. This option allows for tailored solutions if you have specific data retention and restoration needs. Our PS team will work with you to define the scope of the engagement, including the duration of data retention, specific data sets to be restored, and any additional requirements. Please note that bespoke professional services are subject to a separate Fee which will be based on the complexity and duration of the engagement.



8. Decommissioning Process

The decommissioning of the Service will follow the process below:

Cloud Back-up Platform Administration	Us	You
You will submit a termination request in accordance with your MSA. <i>Please note that early termination Fees may apply if you wish to cease your service during the Term.</i>		•
Managed - We will delete all backup agent software/proxy and related components on the source.	•	
Self-Managed - You will delete all backup agent software/proxy and related components on the source.		•
We will delete relevant backup data from our portal, including all backup and recovery schedules, immutable data and backups, encryption keys, and applicable backup data storage. <i>Please note that this process is irreversible once initiated.</i>	•	
We will delete your backup account from our Cloud Back-up platform. <i>Please note that this process is irreversible once initiated.</i>	•	

9. Dependencies

We provide Cloud Back-up Service subject to the following dependencies:

9.1 Client Obligations

- (a) You will ensure that network connectivity from source to target is either procured through us or provided by you in the form of an internet facing connection;
- (b) You will designate a project lead and a technical contact with the appropriate level of expertise to support the successful implementation and operation of the service;
- (c) You will provide all information and configuration details that we may reasonably require to implement the Service;
- (d) You will manage any of your third parties during the implementation and operation of the Service;
- (e) For customers not on Six Degrees Enterprise Cloud, you will ensure that there is sufficient bandwidth capacity for the data to be backed up within your chosen backup windows;
- (f) If you have selected the Self-Service Backup option, you will be responsible for ensuring that your personnel have the relevant technical skills to manage your backup process. We will only provide the initial training courses online as part of the implementation of the Service. We reserve the right to charge an additional Fee for any bespoke training requirement;



- (g) Unless you have selected the Managed Cloud Back-up option, you will be responsible for your own encryption keys. Please note that if you lose your encryption keys, we will not be able to decrypt the backup data;
- (h) Throughout the lifetime of the service, you will be responsible to ensure backup targets have sufficient resources (e.g. RAM, CPU, free disk space) for backups to succeed. Where we provide your selected backup target as part of a different service and you require additional capacity, you can increase the scope of that relevant service subject to an additional Fee; and

9.2 Service Dependencies

- (a) The restore capability of the Service will only be available after an initial full backup of the data is completed.
- (b) Because restores are implemented by the same agent that performs the backups, you will only be able to perform restores on the devices that you have on-boarded to this Service;
- (c) The backup platform requires regular updates, during which time some features may be unavailable. We will use reasonable endeavours to minimise downtime as far as reasonably practicable;
- (d) Please note that, if you are procuring Self-Managed Backups and you wish to elect for a 'compliance mode' deployment (which will provide a hard lockout to our access to your tenant settings and data), you will not be able to reverse this choice;
- (e) It is possible to configure a retention period for backups. As a standard, our retention period is fourteen (14) days. This provides a "grace period" to recover deleted backups. Where you have chosen to opt for a retention period, that the Usage Fees associated to the data used for old backups will not decrease until the retention period has expired.

10. Exclusions

The excluded items described below are outside the scope of this Service Description:

- (a) If you procure our Self-Managed Service, we will not be responsible for any impact to your business due to incorrect configurations, maintenance, or lack of regular monitoring of your backup. We will use reasonable endeavours to escalate any issues that you may experience with the backup platform through 6DG to the relevant vendor, but note that no SLA or operational target will apply.
- (b) The provision of full-OS ("bare-metal") restores is outside the scope of this Service. If you require us to provide such a restore, we will use reasonable endeavours to accommodate your request, but please note that no SLA or operational target will apply.
- (c) We will not be responsible to perform backups or restores on any of your system that is no longer supported by the relevant vendor. In these instances, we will use reasonable endeavours to work with you to find an alternative resolution, but you remain ultimately responsible for ensuring that your systems are supported by the relevant vendor.



11. Definitions and Acronyms

11.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
GB	For the purposes of this document, particularly billing and reporting, a GB is 1,000,000,000 bytes (and does NOT denote a Gibibyte (GiB)).
Protected Server	A server included in the scope of your Service.
Protected Workload	A workload included in the scope of your Service (as set out in your Order Form). Examples of workloads which you may include in your backup plan are virtual machines (VMs), servers, workstations and laptops.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables, and/or timelines for providing services to that client.
Storage	Non-volatile media for storing files, databases, applications, or virtual servers.

11.2 Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
SoW	Statement of Work



12. Operational Targets

Type	P1	P2	P3	P4
Response	30 mins	60 mins	4 hours	Next Business Day
Fix	4 hours	8 hours	16 hours	5 Business Days
Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Description	An issue with the system being backed up/replicated via the Service that meets one of the following conditions, where there is concrete and convincing evidence that our Service is the reason for such problem: • The Cloud Backup portal is not accessible; or • There is substantial degradation of performance, the loss of data, access to the target backup platform or any other materially adverse effect to the source machine or the backup process.	An issue that meets all the following conditions: • It is not a P1 Incident; • It prevents the backup of multiple source machines, or a single source machine over three or more sequential failed backup attempts; and • There is no simple workaround that can enable the backup / replication of, and/or the creation of a replica of, the source workload.	A issue that meets all the following conditions: • It is not a P1 or P2 Incident; • The target backup platform is accessible and available; and • The service is no longer functioning in the way expected. NB: While data restores are P4 requests, failure to restore data due to technical issues with the server may be uplifted to a P3 Incident (or higher if it meets the other criteria).	• Data Restores • Service Requests • Non-service affecting work and reports • A required change or alteration to a service or a technical query • Account administration requests (including password change issues) NB: Where a data restore is required to address an incident under a different Service, the restore will be done as part of that incident, not spun off to a P4 request under this Service.

Please note resolution of incidents related to hardware, software or bandwidth limitations is outside the scope of this Service. Any delay caused by your breach of the obligations set out in Section 9.1 or your failure to meet the dependencies listed in Section 9.2 is excluded from the calculation of our Operational Targets.

Please note that there are no Service Levels or Service Credits associated with the Cloud Back-up Service.