

SPECIFIC CONDITIONS H2 – E-BACKUP MANAGEMENT SERVICES

These Specific Conditions govern the E-Backup Management Services that may be provided by the Company under an Order Form, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms & Conditions for the Supply of Products and/or Services (the “**Conditions**”), which shall be deemed to be incorporated into the Contract for the performance of any E-Backup Management Services performed under these Specific Conditions.

1 DEFINITIONS

- 1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions only:
- | | |
|-------------------------------------|--|
| “Azure” | means the virtual public cloud offering provided by Microsoft called Azure; |
| “Azure Active Directory” | means a multi-tenant directory service from Microsoft that offers authentication, identity management and access capabilities for applications running in Azure together with applications running in an on-premises environment; |
| “Azure Portal” | means the Microsoft owned and managed web browser through which the Customer may access Azure, found at portal.azure.com or any other web browser notified by the Company or Microsoft to the Customer from time to time; |
| “Azure Services” | means the online services within Azure provided by Microsoft to the Customer (if any); |
| “Azure Site Recovery (ASR)” | means Microsoft’s software provided to orchestrate and automate replication of virtual machines between Azure regions; on-premises machines and physical servers to Azure; and/or on-premises machines to a secondary data centre; |
| “Backup Management Services” | means the Services provided in accordance with paragraph 4.1 of these Specific Conditions; |
| “Change” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “Change Management” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “E-Backup Management Services” | means the Services provided by the Company to the Customer in accordance with these Specific Conditions; |
| “Event Management” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “IaaS” | means infrastructure as a service; |
| “Incident” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “Incident Management” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “Microsoft” | means Microsoft Corporation and its affiliates; |
| “Operating System” | means the operating system software that manages the Customer’s computer hardware and software resources and provides common services for software and computer programs to run on the hardware; |
| “PaaS” | means platform as a service; |
| “Problem Management” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “Replication Management Services” | means the Services provided in accordance with paragraph 4.2 of these Specific Conditions; |
| “Recovery Point Objective” or “RPO” | means the maximum allowable amount of lost data measured in time from a failure occurring to the last valid transmission of data from the Customer. It also specifies how far back in time the Customer can go to recover data; |
| “Recovery Time Objective” or “RTO” | means how long it should take to restore data from the time a failure occurred back to an agreed known point in time. It does not include the time required by the Customer to resume normal operations; |
| “Service Management” | has the meaning given to it in Specific Conditions F2 – Service Management; |
| “Service Request” | has the meaning given to it in Specific Conditions X3 – Standard Operational Services; |
| “Supported Cloud Environment” | means any virtual public, private or hybrid cloud environment that is hosting or supporting IaaS, PaaS and/or SaaS for the Customer that may comprise some or all of the following: (i) Azure Services; (ii) DaisyCloud Flex Services, where provided by the Company in accordance with this Contract and/or (iii) cloud services provided by any other third party public or private cloud services provider, and as identified in the Order Form as the Supported Cloud Environment; |
| “Supported Software” | means the Operating System and/or any other software listed as supported software on the Order Form for the purposes of the E-Backup Management Services; and |
| “Subscription” | has the meaning given to it in Specific Conditions I1 – Microsoft Cloud Services. |

- 1.2 All other capitalised terms used in these Specific Conditions that are not defined in paragraph 1.1 have the meanings stated in the Conditions.

2 COMMENCEMENT DATE

- 2.1 The Commencement Date of the E-Backup Management Services shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of the E-Backup Management Services to the Customer.

3 MINIMUM TERM

- 3.1 The Minimum Term shall be the Minimum Term for the E-Backup Management Services as set out in the Order Form or, if no Minimum Term is specified, 12 (twelve) calendar months from the Commencement Date of the E-Backup Management Services.

4 SERVICE DELIVERABLES

4.1 Backup Management Services

- 4.1.1 Where the Company is providing Backup Management Services into or otherwise in connection with the Supported Cloud Environment, as identified on the Order Form it will:
- (a) do so exclusively using technology and software determined by the Company and it reserves the right, at its cost, to change the Backup Management Services technology and/or software from time to time at its sole discretion;
 - (b) implement an agreed backup schedule;
 - (c) perform backups in accordance with the agreed backup schedule;
 - (d) notify the Customer where additional capacity for backups is required;
 - (e) fulfil Backup Management Services administration tasks as follows:
 - (i) monitoring backup progress; and
 - (ii) reviewing backup reports;
 - (f) in the event a backup has failed:
 - (i) use its reasonable endeavours to re-perform the failed backup within the same backup window, subject to backup schedule allowing;
 - (ii) report the failed backup to the Customer; and
 - (iii) investigate the failures in accordance with the Company's Incident Management process. In the event of a repeated failed backup, the Company will initiate Problem Management in accordance with the Company's Problem Management process; and
 - (g) implement Changes to the Backup Management Services in accordance with the Company's Change Management process.
- 4.1.2 Where the Backup Management Services technology and/or software is not expressly agreed to be provided by the Company, backup (capacity and implementation) is the Customer's responsibility.
- 4.1.3 In the event of loss of data that is subject to the Backup Management Services, the Company will restore the data to its last known good status as identified by the Company and notified to the Customer. This activity will be assigned a priority based upon its severity and managed in accordance with the Company's Incident Management process.
- 4.1.4 In the event that restoring the data requires the resources or assistance of the Customer or a third party supplier of the Customer, the Company will manage that third party resource in accordance with the Company's Incident Management and/or Problem Management process, as applicable.
- 4.1.5 The Company will not be responsible for loss or corruption of data, or lack of data consistency, relating to the performance of the Backup Management Services. In circumstances where data is lost or corrupted the Company's liability will be limited to using its reasonable endeavours to restore the previous most recent uncorrupted backup (if available) of such data.

4.2 Replication Management Services

- 4.2.1 Where the Company is providing Replication Management Services into or otherwise in connection with the Supported Cloud Environment, as identified on the Order Form, it will:
- (a) do so exclusively using technology and software determined by the Company and it reserves the right, at its cost, to change the Replication Management Services technology and/or software from time to time at its sole discretion;
 - (b) implement an agreed replication schedule to meet the Customer's RPO and RTO requirements as agreed with the Company;
 - (c) notify the Customer when additional capacity for replication is required;
 - (d) fulfil Replication Management Services administration tasks as follows:
 - (i) monitoring replication progress; and
 - (ii) reviewing replication reports;
 - (e) in the event a replication has failed:
 - (i) use its reasonable endeavours to re-perform the failed replication;
 - (ii) report the failed replication to the Customer;
 - (iii) investigate the failures in accordance with the Company's Incident Management process. In the event of a repeated failed replication, the Company will initiate Problem Management in accordance with the Company's Problem Management process; and
 - (f) implement Changes to the Replication Management Services in accordance with the Company's Change Management process.
- 4.2.2 Where the Replication Management Services technology and/or software is not expressly agreed to be provided by the Company, replication (capacity and implementation) is the Customer's responsibility.
- 4.2.3 In the event of loss of data that is subject to the Replication Management Services, the Company will restore the data to its last known good status as identified by the Company and notified to the Customer. This activity will be assigned a priority based upon its severity and managed in accordance with the Company's Incident Management process.
- 4.2.4 In the event that restoring the data requires the resources or assistance of the Customer or a third party supplier of the Customer, the Company will manage that third party resource in accordance with the Company's Incident Management and/or Problem Management process, as applicable.
- 4.2.5 The Company will not be responsible for loss or corruption of data, or lack of data consistency, relating to the performance of the Replication Management Services. In circumstances where data is lost or corrupted the Company's liability will be limited to using its reasonable endeavours to restore the previous most recent uncorrupted version (if available) of such data.

5 AZURE SPECIFIC CONDITIONS

- 5.1 Where the Company is providing E-Backup Management Services for Azure Services, as identified on the Order Form, the terms in this paragraph 5 shall also apply.

5.2 Azure Site Recovery Management

- 5.2.1 The Company will:
- (a) resolve ASR Incidents in accordance with the Company's Incident Management process;

- (b) implement ASR Changes in accordance with the Company's Change Management process;
- (c) fail over the Azure Services using ASR in the event of a primary site failure; and
- (d) reconfigure the ASR replication to a new secondary site post fail over.

6 REPORTING

- 6.1 The Company will provide the following report where the relevant Service is identified on the Order Form:
- 6.1.1 a Backup Management Services report, providing an overview of the Backup Management Services in the relevant reporting period, including:
- (a) total number of backups;
 - (b) successful backups performed; and
 - (c) failed backups.
- 6.2 All reports provided under this paragraph 6 will be distributed at the relevant frequency aligned to the relevant Service Management tier (as identified on the Order Form). Where no Service Management tier has been identified on the Order Form, the Company will not be obligated to provide any reporting identified in this paragraph 6.

7 CUSTOMER OBLIGATIONS

- 7.1 The Customer will provide or otherwise comply with the following obligations set out in this paragraph 7.1, which are Customer Obligations for the purposes of this Contract:
- 7.1.1 unless otherwise provided by the Company under this Contract, remain responsible for all third party hardware, software, services, subscriptions and/or infrastructure that necessary to enable the provision of the E-Backup Management Services;
 - 7.1.2 ensuring timely participation and engagement with the Change Management process; and
 - 7.1.3 the Customer shall remain responsible for the security and firewalls of the Customer's communications links, equipment, software, services and processes unless agreed otherwise in writing with the Company.

8 EXCLUSIONS

- 8.1 The Company will have no liability (whether in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise) for any failure to provide the E-Backup Management Services (including failing to meet any Service Level), or to pay any Service Credit (if applicable), to the extent caused by any interruption or failure of the E-Backup Management Services arising directly or indirectly as a result of any of the following circumstances set out in this paragraph 8.1:
- 8.1.1 server maintenance or application maintenance carried out by the Customer or a third party;
 - 8.1.2 any failure any act or omission of the third party cloud service provider and/or any other third party provider; and/or
 - 8.1.3 as a result of any delay or failure by the Customer to provide or otherwise comply with the Customer Obligations;
- and the Company reserves the right to levy additional charges on a time and materials basis in respect of such circumstances.
- 8.2 The E-Backup Management Services do not include requests for basic product training or technical consulting.

9 SERVICE LEVELS

- 9.1 The Company will supply the E-Backup Management Services in accordance with the applicable Service Levels set out in Specific Conditions document X3 – Standard Operational Services.

10 CHARGES

- 10.1 The Charges for the E-Backup Management Services are as identified in the Order Form.
- 10.2 The Charges for the E-Backup Management Services will be invoiced monthly in advance, with the first invoice issued by the Company on or around the Commencement Date.