SPECIFIC CONDITIONS I3 – CLOUD MANAGEMENT SERVICES

These Specific Conditions govern the Cloud 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 Cloud 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:

"Active Directory"	means the on-premises Windows Server directory service from Microsoft that stores information about individual members of a domain, including devices and End Users, verifies their credentials and defines their access rights;
"Anti-Virus Management"	means the deployment of anti-virus software utilising the Virus Definitions in accordance with paragraph 4.3 of these Specific Conditions;
"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 Advisor Optimisation Checks"	means the Services provided in accordance with paragraph 6.6 of these Specific Conditions;
"Azure Management Services"	means the Services provided in accordance with paragraph 6 of these Specific Conditions;"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 Security Center Review"	means the Services provided in accordance with paragraph 6.5 of these Specific Conditions;
"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;
"Azure Workload Power Management"	means the Services provided in accordance with paragraph 6.7 of these Specific Conditions;
"Backup Management Services"	means the Services provided in accordance with paragraph 4.4 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;
"Cloud Management Services"	means the Services provided by the Company to the Customer in accordance with these Specific Conditions;
"Critical Patch"	means a Patch designated by the Vendor as 'critical' upon its release or subsequently;
"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;
"Managed Active Directory"	means the Services provided in accordance with paragraph 5 of these Specific Conditions;
"Managed Azure Active Directory"	means the Services provided in accordance with paragraph 6.2 of these Specific Conditions;
"Managed Resource Groups"	means the number of Resource Groups that will be managed by the Company as part of the Cloud Management Services, as set out in the Order Form;
"Managed Subscription Service"	means the Services provided in accordance with paragraph 6.3 of these Specific Conditions;
"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;
"Patch"	means a component of software to fix issues or update computer software or its supporting data;
"Patch Management Service"	means the Services provided in accordance with paragraph 4.2 of these Specific Conditions;
"Problem Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Resource Group"	means any collection of related resources (including virtual machines, databases and other assets) added to Azure, that is created and used to manage permissions, set alerts and manage billing for that collection;
"Security Patch"	means a Patch that is released to address a security related issue;
"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;
"SSL Certificates"	means secure sockets layer (SSL) certificates, which are the small data files that digitally bind a cryptographic key to an organisation's details to enable an encrypted connection between a browser or user's computer and a server or website;
"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 Cloud Management Services;
"Subscription"	has the meaning given to it in Specific Conditions I1 – Microsoft Cloud Services;
"Unmanaged Resource Groups"	means any Resource Group that is not a Managed Resource Group;
"Virus"	means any type of malware, virus, worm, Trojan horse, ransomware, spyware, adware, scareware or other computer program or software code that has been introduced into a system deliberately that carries out a useless and/or destructive function such as displaying an irritating message or systematically over-writing the information stored (that is, "infect" them) and spreads by contact between an infected program and an uninfected program; and
"Virus Definitions"	means the virus definitions provided by the anti-virus software provider as updated from time to time.

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 Cloud 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 Cloud Management Services to the Customer.

3 MINIMUM TERM

3.1 The Minimum Term shall be the Minimum Term for the Cloud 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 Cloud Management Services.

4 SERVICE DELIVERABLES

4.1 **Operating System Support**

4.1.1 The Company will:

(a) monitor Operating Systems in accordance with the Event Management process;

(b) resolve Incidents in accordance with the Incident Management process; and

(c) implement Operating System Changes in accordance with the Change Management process.

4.2 **Patch Management**

4.2.1 Where the Company is providing Patch Management for Supported Software, as identified on the Order Form, it will:

(a) apply Patches to the Supported Software in the Supported Cloud Environment only;

(b) agree a monthly Patching schedule with the Customer for Critical Patches and Security Patches to the Supported Software and deploy all Patches to the Supported Software in accordance with that schedule;

(c) manage the release of Critical Patches and Security Patches remotely as Changes;

(d) when the Change is approved in accordance with the Change Management process, apply the approved Patches to the Customer test environment or test infrastructure according to an agreed Patch schedule;

(e) where a test infrastructure does not exist or the Customer chooses not to have a test environment, use its reasonable endeavours to ensure that a reasonable back-out plan is available. However, the Company will not be liable for any interruption to service in the absence of a test environment or any other unintended consequences, loss or damage caused as a result of such interruption; and

(f) notify the Customer of any Critical Patches and Security Patches that are released that require action outside of the agreed Patching frequency, the installation of which will be managed as Changes.

4.2.2 The Company will provide the Patch Management using Patch Management software determined by the Company. The Company reserves the right to change, at its cost, its Patch Management software from time to time at its sole discretion.

4.3 **Anti-Virus Management**

4.3.1 Where the Company is providing Anti-Virus Management, as identified on the Order Form, it will:

(a) do so exclusively within the Supported Cloud Environment using software determined by the Company and reserves the right to change, at its cost, the anti-virus software from time to time at its sole discretion, unless otherwise agreed in the Order Form; and

(b) undertake the following scanning checks of the servers within the Supported Cloud Environment to seek to detect and clean away Viruses and to help protect files from the Viruses found in the Virus Definitions:

(i) on-access (as files are opened);

(ii) on-demand (a full scan requested as a Service Request); and/or

(iii) scheduled (a full scan at the frequency as set out in the Order Form or as otherwise agreed in writing by the parties);

(c) use reasonable endeavours to help block any Viruses found in the Virus Definitions on detection;

(d) manage and apply updates to the Virus Definitions;

(e) perform configuration of anti-virus software; and

(f) where a Virus is found, take appropriate and reasonable measures to remove the Virus and recover the Operating System as far as reasonably possible to its last known good status as identified by the Company and notified to the Customer.

4.3.2 The Company is not responsible for any data lost or corrupted or rendered inaccessible from the Supported Cloud Environment or otherwise as a result of Virus outbreak or infection, or caused by misuse of any system or application hosted in or connected to the Supported Cloud Environment by End Users or breach by End Users of any security policy.

4.4 **Backup Management Services**

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.4.4 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.

4.4.5 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.

4.5 **SSL Certificates**

Where the Company is managing SSL Certificates in connection with the Supported Cloud Environment, as identified in the Order Form, it will procure and install SSL Certificates from a reputable Certificate Authority, which will be to 2048 bit SSL with 256 bit encryption and SHA2 standard, subject to the Customer paying any third party costs associated with the procurement, renewal or registration process of any additional SSL Certificates.

5 COMPANY SUPPORTED OR MANAGED APPLICATIONS

5.1 **Managed Active Directory**

5.1.1 Where the Company is providing Managed Active Directory, as identified in the Order Form, it will:

(a) monitor the Active Directory in accordance with the Event Management process; and

(b) perform Active Directory administration tasks, as required from time to time in accordance with any relevant Change request from the Customer, comprising the following:

(i) creating computer objects;

(ii) renaming, moving and deleting computer objects within the Active Directory;

(iii) subject to paragraph 5.1.3 managing group policy objects and login scripts;

(iv) clearing local server cache as required;

(v) implementing automated scripts where appropriate; and

(vi) maintaining domain controllers within the domain in accordance with the Company's Active Directory design.

5.1.2 The Company will perform Active Directory routine tasks comprising of the following:

(a) maintaining subnets and sites to support the user login process;

(b) maintaining the global catalogue in the domain;

(c) backing up and recovering Active Directory data; and

(d) implementing Changes to the Active Directory in accordance with the Change Management process.

5.1.3 The Company is not responsible for creating any new Customer group policy objects or changing any Customer group policy objects as part of the Cloud Management Services, unless agreed as an additional Service for additional Charges under this Contract.

6 AZURE SPECIFIC CONDITIONS

6.1 Where the Company is providing Cloud Management Services for Azure Services, as identified on the Order Form, the terms in this paragraph 6 shall also apply.

6.2 **Managed Azure Active Directory**

6.2.1 The Company will:

(a) configure replication between the Customer's Active Directory and the Azure Active Directory utilised for administration and for the Managed Subscription Services;

(b) perform Azure Active Directory administration tasks as required from time to time in accordance with any relevant Change request by the Customer, comprising the following:

(i) managing the Customer's Azure Active Directory replication policy in accordance with Microsoft guidelines;

(ii) restricting permissions for accounts within Azure and Office 365 via role-based administration based upon Microsoft guidelines and built-in roles;

(iii) administering adds, moves and changes to objects within the Azure Active Directory to maintain the working replication necessary between Azure Active Directory and Active Directory; and

(iv) monitoring the replication of information between the Active Directory and Azure Active Directory in accordance with the Event Management process.

6.3 **Managed Subscription Services for Azure**

6.3.1 The Company will perform the following administration tasks:

(a) manage the electronic ordering and administration of Subscriptions relevant to the Azure Services;

(b) manage usage quotas or subscription limits to help ensure suitable availability of resources and capacity within the Azure Services; and

(c) upon request supply the Customer with a reconciliation file of Azure Services usage-based Subscriptions and licence-based Subscriptions for a defined period.

6.3.2 The Customer will not have direct access to the Subscriptions and billing sections of the Azure Portal. The Company may at its discretion from time to time make available to the Customer direct access to a subscriptions and billing portal through a relevant interface. The Customer acknowledges and agrees, that the Company makes no promise, guarantee or commitment to do so, or to maintain access to such portal, if provided.

6.3.3 The Company will hold the administrative rights for the Subscriptions (including the tenancy for such Subscriptions) during the term of the Contract.

6.3.4 The Company will, unless otherwise agreed in writing:

(a) configure Active Directory accounts with read-only role-based access control to the Azure Portal for Managed Resource Groups; and

(b) configure Active Directory accounts with read-write role-based access control to the Azure Portal for Unmanaged Resource Groups.

6.4 **Azure Site Recovery Management**

6.4.1 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.

6.5 **Azure Security Center Review**

6.5.1 Where the Company is providing Azure Security Center Review, as identified on the Order Form, it will:

(a) perform a monthly check of Azure Security Center to review secure score and recommendations made by Azure Security Center;

(b) log all outstanding recommendations as tasks for resolution and assign to the correct resolver group or to the Service Management resolver group; and

(c) where a recommendation requires input from the Customer for reasons of cost, complexity or when considered a project task, raise a task for each recommendation. Service Management will discuss and agree with the Customer which of the recommendations should be progressed and follow the necessary process to allow recommendations to be implemented.

6.6 **Azure Advisor Optimisation Checks**

6.6.1 Where the Company is providing Azure Advisor Optimisation Checks, as identified on the Order Form, it will:

(a) perform a weekly check of Azure Advisor to review recommendations made by Azure Advisor;

(b) log all outstanding recommendations as tasks for resolution and assign to the correct resolver group or to the Service Management resolver group; and

(c) where a recommendation requires input from the Customer for reasons of cost, complexity or when considered a project task, raise a task for each recommendation. Service Management will discuss and agree with the Customer which of the recommendations should be progressed and follow the necessary process to allow recommendations to be implemented.

6.7 **Azure Workload Power Management**

6.7.1 Where the Company is providing Azure Workload Power Management, as identified on the Order Form, it will:

(a) maintain a schedule of workloads and times for power down/power up;

(b) execute automated power down and power ups at specified times;

(c) review the Azure Workload Power Management service monthly with the Customer; and

(d) resolve failures in accordance with Specific Conditions O1 – SSV Management.

7 REPORTING

7.1 The Company will provide the following reports where the relevant Service is identified on the Order Form:

7.1.1 a Patch Management report, providing an overview of Patch Management in the relevant reporting period, including:

(a) status against most recent approved release;

(b) release % success; and

(c) devices below recommended currency;

7.1.2 an Anti-Virus Management report, providing an overview of Anti-Virus Management in the relevant reporting period, including:

(a) items held within the lost and found folder;

(b) decommissioned clients; and

(c) the percentage of devices with the correct version of the anti-virus software; and

7.1.3 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.

7.2 All reports provided under this paragraph 7 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 7.

8 CUSTOMER OBLIGATIONS

8.1 The Customer will provide or otherwise comply with the following obligations set out in this paragraph 8.1, which are Customer Obligations for the purposes of this Contract:

8.1.1 unless otherwise provided by the Company under this Contract, remain responsible for all third party hardware, software, services and/or infrastructure that necessary to enable the provision of the Cloud Management Services;

8.1.2 ensuring timely participation and engagement with the Change Management process;

8.1.3 where the Company is providing Patch Management, the Customer will approve the requests submitted by the Company in accordance with the Change Management process and will not unreasonably withhold or delay such approval; and

8.1.4 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.

9 EXCLUSIONS

9.1 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 Cloud 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 Cloud Management Services arising directly or indirectly as a result of any of the following circumstances set out in this paragraph 9.1:

9.1.1 server maintenance or application maintenance carried out by the Customer or a third party;

9.1.2 any failure any act or omission of the third party cloud service provider and/or any other third party provider; and/or

9.1.3 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.

9.2 The Company does not guarantee the effectiveness of any Virus Definitions. The Company is not responsible for the Virus Definitions not including a specific Virus.

9.3 Non-critical Patches that are required outside the standard monthly patch cycle for critical and security Patches (including feature upgrades and updates) and/or Major version upgrades will be released as agreed with the Customer as additional Services on a chargeable basis.

9.4 The Cloud Management Services do not include requests for basic product training or technical consulting.

10 SERVICE LEVELS

10.1 The Company will supply the Cloud Management Services in accordance with the applicable Service Levels set out in Specific Conditions document X3 – Standard Operational Services.

11 CHARGES

11.1 The Charges for the Cloud Management Services are as identified in the Order Form.

11.2 The Charges for the Cloud Management Services will be invoiced monthly in advance, with the first invoice issued by the Company on or around the Commencement Date.