



SPECIFIC CONDITIONS I4 - DAISY CLOUD PLATFORM

These Specific Conditions govern the Daisy Cloud Services that may be provided by the Company under a Contract, 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 Daisy Cloud Services provided 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 Resiliency"	means as defined in paragraph 4.1.2(a);
"Airgapped"	means a security measure which seeks to ensure that data cannot be accessed via electronic networks or computers;
"Bandwidth"	means an amount of data traffic measured in b/s (bits per second) across the inter-connect;
"Basic Backup Solution"	means an automated backup solution for the Customer Environment and the Customer's data within the Customer Environment that will comprise daily backups that will be retained for 31 (thirty one) days or such other period as set out in the Order Form;
"Broadband Acceptable Use Policy"	means the Company's policy for the acceptable use of its Broadband Services and/or the internet, the current version of which is available at www.daisyuk.tech (or at such other website address as is notified to the Customer by the Company from time to time);
"Change Management"	has the meaning given to it in Specific Conditions X3 – Standard Operational Services;
"Customer Data"	means all data, including all text, sound, video, image files and software that are provided to the Company by, or on behalf of, the Customer through use of the Daisy Cloud Services;
"Customer Environment"	means the agreed service elements for the Daisy Cloud Platform for the Customer as set out in the Order Form;
"Daisy Cloud Network"	means the Daisy Cloud Hardware, excluding the storage and servers;
"Daisy Cloud Platform"	means together the Daisy Cloud Hardware and the Hypervisor provided by the Company and made available to the Customer to host virtual services which includes VMWare hypervisor licensing and host based Microsoft Windows server operating system licensing;
"Daisy Cloud Services"	means the provision of the Daisy Cloud Platform by the Company to the Customer for hosting the Customer Environment together with any and all Services provided by the Company under these Specific Conditions;
"Daisy Cloud Hardware"	means the hardware, including but not limited to the relevant storage and servers, switches, routers and firewalls owned and provided by the Company to support the Daisy Cloud Services;
"DNS"	means domain name system, which is the Internet's system for converting alphabetic names into numerical IP addresses;
"Hypervisor"	means software that runs on computer hardware that allows one or more host computers to support multiple guest virtual machines by virtually sharing its resources;
"Immutability Period"	means the period during which data is rendered Immutable;
"Immutable Storage"	means a chargeable upgrade to the Basic Backup Solution which may include any combination of: local, remote or offsite Airgapped configuration as identified in the Order Form;
"Immutable" or "Immutability"	means stored data that cannot be changed or deleted;
"Incident"	means as defined in Specific Conditions X3 - Standard Operational Services;
"Incident Management"	means as defined in Specific Conditions X3 - Standard Operational Services;
"Intersite Service"	means (if any stated on the Order Form) the connectivity between a Primary Data Centre and a Secondary Data Centre provided in accordance with paragraph 6;
"IP"	means internet protocol, which is the method or protocol by which data is sent from one computer to another on the internet;
"Public IP Address"	means internet protocol address, which is the unique identifier for a computer or other device that distinguishes it from all other devices connected to the internet;
"IP-SEC VPN"	means IP security virtual private networks, being the set of protocols that provides security for IPs used for setting up of virtual private networks (VPNs) in a secure manner;
"ISP"	means an internet service provider;
"Measurement Period"	means as defined in paragraph 13.3;
"Network Time Protocol"	means a protocol used to synchronize computer clock times in a network;
"Non-Active Resiliency"	means as defined in paragraph 4.1.2(b);
"Primary Data Centre"	means the data centre facility used as the primary location housing the Daisy Cloud Platform;
"Quality of Service"	means the capability of a network to provide better service to selected network traffic over various technologies, including frame relay, asynchronous transfer mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies;
"Recovery Point Objective"	means the age of files that would be recovered from backup storage for normal operations to resume if the Daisy Cloud Platform is affected by a disaster or disruption, as set out in the Order Form;
"Recovery Time Objective"	means the targeted duration of time within which the Daisy Cloud Platform would be restored after a disaster or disruption, as set out in the Order Form or the design document;
"Resiliency Options"	means the resiliency options for the Daisy Cloud Services (if any) as set out in the Order Form;
"Secondary Data Centre"	means (if any set out in the Order Form) the data centre facility used as a secondary data centre, which may be designated to act as a failover for any occurrence where Services from the Primary Data Centre are compromised;
"Service Availability"	means the proportion of time that the Daisy Cloud Platform is available during the Measurement Period as defined and calculated in accordance with paragraph 13.2;
"Service Management"	means the Services described in Specific Conditions F2 – Service Management;
"Scheduled Maintenance"	means any maintenance, planned outages or server relocation scheduled by the Company (which for the avoidance of doubt does not include patching and/or software and/or firmware upgrades) in accordance with paragraph 9.
"SQL"	means structured query language, which is the standard computer language for relational database management and managing data;
"VLAN"	means a virtual local area network, which is any broadcast domain that is partitioned and isolated in a computer network at the data link layer;



"VRF" means virtual routing and forwarding, which is a technology included in IP network routers that allows multiple instances of a routing table to exist in a router and work simultaneously; and

"WAN" means wide area network, which is a telecommunications network or computer network that extends over a large geographical distance.

1.2 All other capitalised terms that are not defined in paragraph 1.1 shall have the meanings stated in the Conditions.

2 COMMENCEMENT DATE

2.1 The Commencement Date of the Daisy Cloud 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 the provision of Daisy Cloud Services to the Customer.

3 MINIMUM TERM

3.1 The Minimum Term shall be as set out in the Order form, or if no Minimum Term is specified, twelve (12) calendar months from the Commencement Date.

4 DAISY CLOUD PLATFORM

4.1 The Company will:

- 4.1.1 maintain the Daisy Cloud Hardware within a Primary Data Centre and if required to support resiliency in accordance with paragraph 4.1.2 and (if set out in the Order Form) a Secondary Data Centre;
- 4.1.2 provide the Daisy Cloud Platform to support the Customer Environment as set out in the Order Form, together with the following Resiliency Options (if any) as set out in the Order Form:
 - (a) if Active Resiliency is set out in the Order Form, the Company will:
 - (i) provide a live instance of the Customer Environment in a Secondary Data Centre to mirror the live instance of the Customer Environment in the Primary Data Centre, together with the Intersite Services in accordance with paragraph 6; and
 - (ii) failover and restore the Customer Environment into a Secondary Data Centre in accordance with the Recovery Time Objective for Active Resiliency;
 - (b) if Non-Active Resiliency is set out in the Order Form, the Company will:
 - (i) provide a standby replicated copy of the Customer Environment, together with the Intersite Services in accordance with paragraph 6;
 - (ii) provide the relevant licences for the necessary replication software; and
 - (iii) failover and restore the Customer Environment into a Secondary Data Centre in accordance with the Recovery Time Objective for Non-Active Resiliency;
 - (c) Where specified on the Order Form that the Company is providing a Resiliency Option, the Company will:
 - (i) provide and maintain a service continuity management plan for a pre-determined and agreed level of service to support the minimum business requirements of the Customer following a business service interruption to the Customer Environment;
 - (ii) where the Customer has chosen a Resiliency Option, provide plans that endeavour to meet the Recovery Time Objective and Recovery Point Objective levels.
- 4.1.3 provide termination points into a Primary Data Centre and (if applicable) a Secondary Data Centre for the Customer's WAN connectivity;
- 4.1.4 where required and identified in the Order Form, provide IP-Sec VPN on Company provided and managed firewalls, for third party remote access (providing always that the Customer accepts it is liable for and shall hold the Company harmless against all costs, losses and liabilities caused by the acts and omissions of the applicable third party whilst it accesses the Daisy Cloud Services);
- 4.1.5 where required and identified in the Order Form, provide two-factor authentication, for third party remote access (providing always that the Customer accepts it is liable for and shall hold the Company harmless against all costs, losses and liabilities caused by the acts and omissions of the applicable third party whilst it accesses the Daisy Cloud Services);
- 4.1.6 where required and identified in the Order Form, deploy a Basic Backup Solution. These back-ups will not be retained following termination or expiry of the Contract;
- 4.1.7 where required and identified in the Order Form, provide Immutable Storage for the Immutability Period;
- 4.1.8 provide the Third Party Software licensed products stated in the Order Form as being provided by the Company as part of the Daisy Cloud Services (providing always that the Customer hereby acknowledges and agrees that it shall not use such licences except within the Daisy Cloud Services);
- 4.1.9 apply patches and/or firmware updates to the Daisy Cloud Hardware and Hypervisor to address security vulnerabilities without undue delay following the release of the security patches and/or relevant updates from the relevant Vendor and the Customer acknowledges and agrees that the Company shall not otherwise be obliged to patch the Customer's operating systems or software on the Daisy Cloud Platform unless such obligation is expressly accepted by the Company in an Order Form with reference to Specific Conditions I3 – Cloud Management Services;
- 4.1.10 where required and identified in the Order Form, provide an internet breakout service, under which the Company will:
 - (a) provide secure internet connectivity to each server within a Primary Data Centre and (if applicable) a Secondary Data Centre via independent diversely routed switches and routers;
 - (b) monitor and manage this service;
 - (c) provide public IP Addresses; and
 - (d) provide and maintain logical segregation of networks on shared infrastructure using VLAN separation, unique subnets and WAN VRF separation as appropriate;
- 4.1.11 provide a data centre network management service, under which the Company will:
 - (a) manage a secure data transmission local area network service within a Primary Data Centre and (if applicable) a Secondary Data Centre;
 - (b) monitor and manage the Daisy Cloud Network 24x7; and
 - (c) provide and maintain logical segregation of networks on shared infrastructure using VLAN separation, unique subnets and WAN VRF separation as appropriate.
- 4.1.12 provide a storage management service, under which the Company will:
 - (a) provide the relevant amount of storage as specified in the Order Form on the Daisy Cloud Platform; and
 - (b) manage the storage arrays and fibre interconnects.
- 4.1.13 undertake contingency, backup and recovery strategy planning for the Daisy Cloud Platform for the provision of a continued service in respect of both Active Resiliency and Non-Active Resiliency following a business service interruption to the Daisy Cloud Platform.
- 4.2 The Daisy Cloud Services are provided solely for the Customer's use and the Customer may not resell or attempt to resell the Daisy Cloud Services (or any part of them) to any third party.
- 4.3 The Company reserves the right (at the Company's sole discretion):
 - 4.3.1 to make changes to the Daisy Cloud Services (or any part thereof) that do not have a material adverse effect on the Services and shall where the Company deems it practical to do so, give the Customer notification of the same;



- 4.3.2 to suspend access to all or any part of the Daisy Cloud Services if at any time the Company has reasonable grounds to suspect that there has been or is likely to be a breach of security; and/or
- 4.3.3 to require the Customer to (in which case, the Customer shall) change any or all of the passwords the Customer uses in connection with the Daisy Cloud Services.
- 4.4 Where the Company agrees to supply any IP Addresses, as expressly stated in the Order Form:
 - 4.4.1 any such IP Address that may be supplied by the Company to the Customer is licensed to the Customer on a non-exclusive, non-transferable, revocable basis for use only in conjunction with the Daisy Cloud Services and will remain the Company's or its licensor's property;
 - 4.4.2 following disconnection of the Daisy Cloud Services the Customer's licence to use any IP Address supplied by the Company will automatically terminate; the Customer will not make any further use of it (unless otherwise agreed in writing); and it may be re-assigned by the Company either to the Company itself or to a third party; and
 - 4.4.3 the Company reserves the right to charge the Customer for any IP Address used or retained by the Customer after termination of this Contract.

5 CUSTOMER DATA

- 5.1 As between the parties, the Customer retains all right, title and interest in and to Customer Data. The Company does not acquire any rights in Customer Data, other than the rights that the Customer grants to the Company under this Contract for it to provide the Daisy Cloud Services to the Customer. The Customer Data will be used or otherwise processed by the Company only to provide the Daisy Cloud Services to the Customer, including purposes compatible with providing those Services. The Company will not use or otherwise process any Customer Data or derive information from it for any advertising or similar commercial purposes.
- 5.2 The Company will not disclose Customer Data outside of its Group or subcontractors except:
 - 5.2.1 as the Customer directs;
 - 5.2.2 as described in this Contract; or
 - 5.2.3 as required by law.
- 5.3 Customer Data may include Protected Data provided to the Company by, or on behalf of, the Customer through use of the Daisy Cloud Services. To the extent the Company is a processor or sub-processor of Protected Data subject to the Data Protection Laws, the terms in clause 16 of the Conditions govern that processing and the parties also agree to the following terms in this paragraph 5.
- 5.4 The parties agree that the Customer is the controller of Customer Data that is Protected Data and the Company is the processor of such data, except:
 - 5.4.1 when the Customer acts as a processor, in which case the Company is a sub-processor; or
 - 5.4.2 as expressly stated otherwise in this Contract.
- 5.5 The Customer agrees that the terms of this Contract are the Customer's complete and final documented instructions to the Company for the processing of Protected Data. Any additional or alternate instructions must be agreed to as a Variation to this Contract in accordance with the Conditions.
- 5.6 The parties agree that the Company is the data controller for business contact information or other Personal Data that may be collected at the same time as Customer Data but is needed by the Company to maintain the business relationship with the Customer.
- 5.7 All rights to access or use the Daisy Cloud Services will terminate upon termination or expiry of the Daisy Cloud Services under this Contract, save as otherwise agreed between the parties. Except as otherwise expressly agreed between the parties in writing, the Customer will not have access to any Customer Data following expiry or termination of this Contract. At the Customer's choice, which shall be made and notified in writing to the Company prior to expiry or termination, the Company will delete or return to the Customer all the Customer Data after the end of the provision of Services, and delete existing copies unless Relevant Law requires storage of the Personal Data. In the absence of the notification of the Customer's choice being received by the Company prior to the expiry or termination of the Contract, the Company shall be entitled to delete all copies of the Customer Data.
- 5.8 The expiration or termination of the Daisy Cloud Services will not prejudice the Customer's obligation to pay for the storage (if any) of Customer Data agreed between the parties in writing.
- 5.9 Without prejudice to the Company's rights of suspension in the Conditions, the Company may (but shall not be obliged to) suspend the Customer's use of the Daisy Cloud Services if:
 - 5.9.1 it is reasonably needed to prevent unauthorised access to Customer Data;
 - 5.9.2 the Company believes that the Customer or the Customer Data breaches Relevant Law;
 - 5.9.3 the Customer fails to respond to a claim of alleged infringement of third party Intellectual Property Rights under paragraph 5.12 within a reasonable time; and/or
 - 5.9.4 the Customer does not abide by the Acceptable Use Policy or violates any other term of these Specific Conditions;

and such suspension will apply to the minimum necessary part of the Daisy Cloud Services and will be in effect only while the condition or need exists. The Company will give notice before any such suspension, except where it reasonably believes it needs to suspend immediately. If the Customer does not fully address the reasons for the suspension within 60 (sixty) days after suspension, the Company may terminate the Daisy Cloud Services and delete the Customer Data without any retention period.
- 5.10 Both parties agree to fully co-operate with the Police and any other relevant authorities (including but not limited to HM Revenue and Customs, Trading Standards, the Information Commissioner's Office and/or OFCOM and their successors from time to time) in connection with any Customer Data and/or misuse or suspected misuse of the Daisy Cloud Services, and the Customer consents to the Company co-operating with any such authority and with any other telecommunications operators in connection with the Daisy Cloud Services if the Company is required to do so by law. If any such authority contacts the Company with a demand for Customer Data, the Company will attempt to redirect the third party to request that data directly from the Customer. The Customer agrees without prejudice to the generality of the foregoing, that the Company will be entitled to divulge any information that the Company holds that may be relevant to any investigation, including the name, address and account information relating to the Customer to such third parties.
- 5.11 Any assistance given by the Company in relation to any fraudulent and/or unauthorised use by the Customer and/or third parties (or the prevention of such use) will be on a reasonable endeavours basis only and no liability can be accepted by the Company for any loss sustained by the Customer arising from fraudulent and/or unauthorised means that are beyond the Company's reasonable control (save for any fraud and/or unauthorised use by an employee, agent or contractor of the Company acting in that capacity).
- 5.12 Subject to clause 19.9 of the Conditions, the Customer shall indemnify the Company and keep the Company indemnified against all losses, damages, reasonable costs or reasonable expenses and other liabilities (including reasonable legal fees) incurred by, awarded against or agreed to be paid by the Company arising from any claim made against the Company for actual or alleged infringement of a third party's Intellectual Property Rights arising out of the Customer Data or any processing, storage or other necessary use in accordance with this Contract by the Company of such Customer Data in conjunction with the Daisy Cloud Services.

6 INTERSITE SERVICE

- 6.1 Where the Company is providing an Intersite Service as identified in the Order Form, it will:
 - 6.1.1 provide a secure connection between a Primary Data Centre and a Secondary Data Centre via independent diversely routed switches and routers;
 - 6.1.2 monitor and manage the Intersite Service;
 - 6.1.3 provide and maintain logical segregation of networks on shared infrastructure using VLAN separation, unique subnets and WAN VRF separation;
 - 6.1.4 provide Quality of Service options (if any) as set out in the Order Form; and
 - 6.1.5 provide the allocated Bandwidth detailed in the Order Form.

7 SOFTWARE LICENCE TERMS



- 7.1 To the extent that the Daisy Cloud Services involve End Users accessing Software then the Customer shall procure that all End Users shall comply with the applicable licence terms, not cause the Customer to breach such terms and provide the Company with such necessary registration details as are to be agreed between the Company and the Customer, which will be a minimum of the End User's full name and email address. The Customer acknowledges and accepts that if the End User does not provide this information and does not agree to any relevant acceptable use terms and conditions relating to such Software as notified by the Company from time to time in writing then the End User will not be able to connect to the applicable Software.

- 7.2 The Customer acknowledges and accepts that the Company shall have no liability to the Customer to the extent that the End User is unable to access the relevant Software and/or Daisy Cloud Services to the extent due to any failure to provide the necessary information set out in paragraph 7.1.

8 THIRD PARTY SOFTWARE AND LICENCES

- 8.1 As part of the Daisy Cloud Services, the Customer may be permitted to use certain Third Party Software developed and owned by Vendors. If the Customer uses the Third Party Software, the Customer agrees to these additional terms and conditions:

- 8.1.1 the Third Party Software is neither sold nor distributed to the Customer and the Customer shall use it solely as part of the Daisy Cloud Services;
- 8.1.2 the Customer shall not transfer or use the Third Party Software outside the Daisy Cloud Services;
- 8.1.3 the Customer shall not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Third Party Software; and
- 8.1.4 the Customer shall not reverse engineer, decompile or disassemble the Third Party Software, except to the extent expressly permitted by applicable law.

- 8.2 The Customer acknowledges and agrees that the Vendors disclaim, to the extent permitted by applicable law, all warranties by the Vendors and any liability by the Vendors or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Daisy Cloud Services and/or the provision of the Third Party Software in relation to such Services. The Customer acknowledges and agrees that the Vendors are not responsible for providing any support in connection with the Services and/or the Third Party Software. The Customer shall not contact the Vendors for such support.

- 8.3 The Customer acknowledges and agrees that the Company disclaims, to the extent permitted by applicable law, all warranties by the Company and any liability by the Company for any damages, whether direct, indirect, or consequential, arising from the provision or use of the Third Party Software in relation to the Daisy Cloud Services.

- 8.4 The Customer acknowledges and agrees that it is not granted any right to use the Third Party Software in any application controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, weaponry systems, or any similar scenario (collectively, "**High Risk Use**"). The Vendors and their suppliers disclaim any express or implied warranty of fitness for High Risk Use. High Risk Use does not include utilisation of the Third Party Software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function.

9 SCHEDULED MAINTENANCE

- 9.1 Subject to paragraphs 9.2 and 9.3, Scheduled Maintenance on the Daisy Cloud Platform and on the Primary Data Centre or Secondary Data Centre (excluding emergency maintenance) will be provided by the Company to the Customer and the Company will use its reasonable endeavours to carry out such Scheduled Maintenance during the period from 12.01am on a Saturday to 11.59pm on a Sunday

- 9.2 To the extent the Daisy Cloud Services include provision of a Secondary Data Centre, the Company will ensure that Scheduled Maintenance does not occur at both the Primary Data Centre and the Secondary Data Centre during the same scheduled maintenance period. Outside of the scheduled maintenance period, as permitted in accordance with paragraph 9.1, the Company may undertake maintenance activities provided that there is no impact on the Service Availability of the Daisy Cloud Platform.

- 9.3 The Company will provide to the Customer as much advance notice as is reasonably practicable (in any event no less than 5 (five) Business Days' notice) of any Scheduled Maintenance.

10 REPORTING

- 10.1 Subject to clause 10.2, the Company will provide reporting on Service Availability monthly.

- 10.2 The frequency of the reporting will be aligned to the Service Management tier purchased by the Customer from the Company and identified in Specific Condition F2 – Service Management. Where Service Management is not procured by the Customer from the Company, the Company shall not be obligated to provide the reporting.

11 CUSTOMER OBLIGATIONS

- 11.1 The Customer is responsible for:

- 11.1.1 determining whether the Daisy Cloud Services are appropriate for storage and processing of information subject to any specific law or regulation applicable to the Customer and/or the Customer's industry and for using the Daisy Cloud Services in a manner consistent with Customer's legal and regulatory obligations;
- 11.1.2 for responding to any request from any regulatory authority regarding Customer's use of the Daisy Cloud Services, such as a request to delete or take down content under Relevant Laws;
- 11.1.3 ensuring there is no fraudulent and/or unauthorised use of the Daisy Cloud Platform or any use by any unauthorised third parties (who are not employees of the Customer or the Customer's Group) that would constitute a breach by the Customer of its obligations under this Contract;
- 11.1.4 providing the Company with all information and documentation that may reasonably be requested by the Company in order to allow the Company to fulfil its obligations;
- 11.1.5 maintaining the security and firewalls of the Customer's systems, network elements, communications links, equipment, software, services and processes used in connection with the Daisy Cloud Services, unless expressly agreed otherwise in this Contract;
- 11.1.6 maintaining (and ensuring that each of its authorised End Users maintains) at all times, the integrity and secrecy of all passwords, log-in details and access codes used for the purposes of accessing of using the Daisy Cloud Services;
- 11.1.7 providing all licensing of all software that is not set out in the Order Form as being provided by the Company;
- 11.1.8 support for any application running on the Daisy Cloud Platform that is not otherwise expressly agreed to be maintained by the Company under this Contract;
- 11.1.9 ensuring that the Customer's employees adhere to the Customer's Broadband Access Usage Policy;
- 11.1.10 the replacement costs associated with the loss, damage or renewal to any token provided as part of two-factor authentication provided by the Company;
- 11.1.11 defining and enforcing local End User policy on acceptable data for storage and backup purposes and advising the Company of that policy as amended from time to time;
- 11.1.12 timely engagement with the Company's Change Management process;
- 11.1.13 any and all data held on devices that have not been synchronised with the Daisy Cloud Platform;
- 11.1.14 save to the extent it is agreed in writing by the Company to do so, the back-up of any Customer Data stored in the Daisy Cloud Platform; and
- 11.1.15 the secure storage, management and provision of restores of any data backed up prior to the Commencement Date.

- 11.2 The Customer agrees and undertakes:

- 11.2.1 not to use the Daisy Cloud Services to send, receive or store any material that could constitute or encourage conduct that would be considered a criminal offence; or that is either offensive, abusive, indecent, obscene, pornographic, fraudulent, libellous, defamatory, menacing, criminal or likely



- 11.2.2 to cause annoyance or distress to any third party or likely to incite or promote illegal activities in any jurisdiction and to otherwise use the Daisy Cloud Services in accordance with Relevant Laws and in a manner that does not cause the Company to breach any Relevant Laws;
- 11.2.3 not to use the Daisy Cloud Services in a manner that constitutes a violation or infringement of the rights (including, without limitation, any Intellectual Property Rights) of any other person;
- 11.2.3 to implement adequate control and security over the use of the Daisy Cloud Services by its End Users, including but not limited to the prevention of Viruses; and
- 11.2.4 not to cause, aid, encourage or facilitate a domain or URL hosted by the Company for the Customer to point or otherwise direct traffic to any material that violates any Relevant Laws.

12 EXCLUSIONS

- 12.1 The following are expressly excluded from the scope of the Daisy Cloud Services and these Specific Conditions:
 - 12.1.1 administrative access for the Customer to Daisy Cloud Platform;
 - 12.1.2 any software licence renewals and/or security certificate renewals, save as expressly provided in these Specific Conditions or otherwise provided in the Order Form;
 - 12.1.3 any security services and therefore the Company will not be liable for any security-related attacks or impact that causes any loss to the Customer;
 - 12.1.4 the encryption of any Customer Data unless otherwise expressly agreed;
 - 12.1.5 the provision of any assistance or services in relation to the Customer's migration or transfer to the Daisy Cloud Services, which may be provided in addition, where expressly stated in the Order Form, subject always to Specific Conditions X2 – Professional Services;
 - 12.1.6 the provision of firewalls and/or local area network services, which may be provided in addition, where expressly stated in the Order Form, subject always to Specific Conditions G1 – Local Area Network Services;
 - 12.1.7 the provision of cloud management services, which may be provided in addition, where expressly stated in the Order Form, subject always to Specific Conditions I3 – Cloud Management Services; and
 - 12.1.8 the provision of connectivity services, which may be provided in addition, where expressly stated in the Order Form, subject always to Specific Conditions J1 – Connectivity Services.

13 SERVICE LEVELS

13.1 Incident Management Service Levels

The Company will provide Incident Management in accordance with the Service Levels set out in Specific Conditions X3 – Standard Operational Services.

13.2 Service Availability

- 13.2.1 The target minimum Service Availability for the Daisy Cloud Services is as set out in the Order Form. Service Availability is calculated in accordance with paragraph 13.2.2..
- 13.2.2 Subject to paragraph 13.4, the Service Availability of the Daisy Cloud Services is measured as a percentage and is a representation of the portion of time that the relevant service is available during the Measurement Period calculated in accordance with this paragraph 13.2.2.

Availability is calculated using the following formula:

$$\text{Availability} = \frac{(AST - DT)}{AST} \times 100$$

Where:

AST = Agreed Service Time (which unless otherwise agreed is the total number of minutes in the Measurement Period)

DT = Downtime being the actual time in minutes that the Daisy Cloud Platform is unavailable during the Agreed Service Time

13.3 Measurement Period

Unless otherwise stated in the Order Form, the Company's performance against the Service Levels will be measured each calendar month on the first day of the calendar month following the Commencement Date (the "Measurement Period"). Save in the case of manifest and demonstrable error, the Company's performance against the Service Levels shall be based solely on information recorded by the Company.

13.4 Service Level Exclusions

- 13.4.1 Any downtime or unavailability of the Daisy Cloud Services to the extent caused by the following shall be deemed not to be downtime for the purposes of the calculation of the Service Availability in accordance with paragraph 13.2 and the following shall not be taken into account for the purposes of any other Service Level calculations and such matters shall not be counted or considered in relation to any performance by the Company of any Service Level or other term or condition of this Contract:
 - (a) individual server or infrastructure component failure where the Daisy Cloud Services remain available (for example, the failure of a single web server in load balanced configuration while the alternate remains in service);
 - (b) where any third party application software becomes unsupported for reasons outside of the Company's control or any issues relating to third party application software that require the third party Vendor to remedy the issue;
 - (c) any hardware/software or communication link fault or failure at the Customer Premises or other Site (where such equipment is not otherwise owned and managed by the Company);
 - (d) incidents to the extent caused by issues affecting any connectivity services that are outside of the Daisy Cloud Services;
 - (e) any emergency maintenance carried out and/or any Scheduled Maintenance carried out in accordance with paragraph 9;
 - (f) any downtime that is caused by the Customer or by a third party that is not a sub-contractor of or otherwise controlled or managed by the Company;
 - (g) where a Primary Data Centre and Secondary Data Centre forms the Daisy Cloud Services, any downtime of a Primary Data Centre or Secondary Data Centre where the other data centre and other Daisy Cloud Services remain available;
 - (h) any downtime or incident to the extent arising due to the invocation of an agreed exit plan or transitional assistance during the termination period.
- 13.4.2 The Company will provide the Customer with details of any exclusions claimed as part of its service reports to the Customer where Service Management has been procured from the Company.

14 CHARGES

- 14.1 The Charges for the Daisy Cloud Services are as set out in the Order Form.
- 14.2 Unless otherwise provided in the Order Form, the Company will invoice the Charges for the Daisy Cloud Services monthly in advance.