Reference SSC-MDMS-001
Dated 26th February 2018

Service Specific Conditions for the supply of the Daisy Device Management Service which apply in addition to (and which supplement and/or vary):

Daisy Terms and Conditions for the Provision of Equipment and/or Mobile Network Services – October 2014 ("*Mobile Terms and Conditions*")

A. Terms and conditions which apply in addition to the Mobile Terms and Conditions

1. **Definitions**

1.1 "Daisy Device Management Service" means the software as a service offering provided by the Company more particularly described in Schedule 1 to these Service Specific Conditions;

1.2 "Device(s)" means any mobile communication device on which the Daisy Device Management Service is to be installed, including without limitation any tablet, smartphone, mobile telephone or netbook;

1.3 "Mobile Network Services" includes the provision to the Customer of the Daisy Device Management Service;

1.4 "Service Operator" means any mobile network operator and/or any of the Company's licensors;

1.5 "Tariff" means, in respect of the Daisy Device Management Service, the rate card set out in Schedule 2 to these Service Specific Conditions; and

1.6 "User Subscriptions" means the user subscriptions purchased by the Customer pursuant to paragraph 2.1 below which entitle End Users to access and use the Daisy Device Management Service in accordance with this Contract.

2. **Access to, and use of, the Daisy Device Management Service**

2.1 Following the purchase of the relevant quantity of User Subscriptions by the Customer, the Company shall grant to the Customer a non-exclusive, non-transferable right to permit the End Users to use the Services during the term of the Contract solely for the Customer's internal business operations.

2.2 The Customer, and not Daisy, shall:

2.2.1 obtain and maintain all Device and computer hardware, software and communications equipment and services needed to access the Daisy Device Management Service; and

2.2.2 Install the Daisy Device Management Service on its authorised users' Devices.

2.3 The Customer undertakes that:

2.3.1 it will not allow or suffer any User Subscription to be used by more than one individual End User unless it has been reassigned in its entirety to another individual End User, in which case the prior End User shall no longer have any right to access or use the Daisy Device Management Service;

2.3.2 it shall maintain a written, up to date list of authorised End Users and provide such list to the Company within five (5) Business Days of the Company's written request at any time or times;

2.3.3 it shall permit the Company to audit the Customer's use of the Daisy Device Management Service in order to confirm the Customer's proper use of it. Such audit may be conducted no more than once per quarter, at the Company's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Customer's normal conduct of business;

2.3.4 if any audit referred to in paragraph 2.3.3 reveals that any password has been provided to any individual who is not an End User, then without prejudice to the Company's other rights, the Customer shall promptly disable such passwords and the Company shall not issue any new passwords to any such individual;

2.3.5 to pay the applicable charges if the Customer authorises additional User Subscriptions or Devices to use the Daisy Device Management Services (for example via a Daisy internet portal); and

2.3.6 if any audit referred to in paragraph 2.3.3 reveals that the Customer has underpaid Charges to the Company, then without prejudice to the Company's other rights, the Customer shall pay to the Company an amount equal to such underpayment as calculated in accordance with the Charges set out in paragraph 2 of these Service Specific Conditions within ten (10) Business Days of the date of the relevant audit.

2.4 From time to time, upon reasonable notice to the Customer, and for the purpose of enhancing the performance and functionality of the Daisy Device Management Service, the Company may make additions, deletions, and modifications to the underlying networks, access points' applications and other facilities in connection with the Daisy Device Management Service, and automatic updates to Daisy Device Management Service, such as directory updates, and "bug" fixes. The Customer shall upgrade to the latest version of the Daisy Device Management Service within twelve (12) months of a new release.

2.5 The Company retains the right to change the Daisy Device Management Service, or with reasonable written notice, cause the Customer to migrate to the most recent version of the Daisy Device Management Service, at its sole discretion. In the event a failure of the Daisy Device Management Services to conform to the Specification, in Schedule 1, the Customer shall provide to the Company reasonably detailed documentation and explanation, together with underlying data, to substantiate any such failures and shall assist the Company in its efforts to investigate, diagnose and correct the failure. The Company and the Customer shall make commercially reasonable efforts to work together in order to troubleshoot, support, and work to resolve issues which occur in each environment.

3. **Obligations of the Customer**

3.1 The Customer (and not the Company) shall carry out any and all installation activities necessary on each Device to enable the Customer and the End Users to utilise the Daisy Device Management Service on that Device.

3.2 The Customer shall co-operate with the Company in all matters relating to the Daisy Device Management Service.

3.3 Notwithstanding paragraph 3.2, the Customer shall comply with any reasonable instructions issued by the Company relating to the Daisy Device Management Service and shall only use Devices approved by the Service Operators and the British Approvals Board of Telecommunications.

3.4 The Customer shall provide to the Company, in a timely manner, all information as the Company may reasonably require for the purposes of performing its obligations under this Agreement.

3.5 The Customer shall not be involved, directly or indirectly, or knowingly, recklessly or negligently permit any other person to be involved, in any fraud, unlawful, illegal or immoral activity in connection with the Customer's use of the Daisy Device Management Service and shall notify the Company immediately upon becoming aware of any such activity.

3.6 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Daisy Device Management Service and, in the event of any such unauthorised access or use, promptly notify the Company.

3.7 The Customer shall not:

3.7.1 except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under this Contract:

3.7.1.1 copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of any software which constitutes the Daisy Device Management Service in any form or media or by any means;

3.7.1.2 reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of any software which constitutes the Daisy Device Management Service; or

3.7.1.3 merge the Daisy Device Management Service with any other software, products or services;

3.7.2 access all or any part of the Daisy Device Management Service in order to build a product or service which competes with the Daisy Device Management Service;

3.7.3 use the Daisy Device Management Service to provide services to third parties;

3.7.4 license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Daisy Device Management Service available to any third party other than the End Users;

3.7.5 access or attempt to access the account of any third party (not including the End Users) which also uses the Daisy Device Management Service, or to breach or attempt to breach the Company's or any third party's IT security protections;

3.7.6 use the Daisy Device Management Service:

3.7.6.1 to breach any applicable law or regulation or in a way which is libellous, defamatory, indecent, obscene or pornographic;

3.7.6.2 to infringe the copyright, trademark, trade secret or other intellectual property right of any third party;

3.7.6.3 to interfere with other users' use of the Daisy Device Management Service or of the internet;

3.7.6.4 to collect or attempt to collect personal information about third parties without their consent; or

3.7.6.5 for the online control of nuclear facilities, aircraft navigation systems, aircraft communication systems, air traffic control, to direct life support machines or weapon systems.

4. Obligations of the Company

4.1 The Company shall provide the Daisy Device Management Service substantially in accordance with the Specification at Schedule 1 and with reasonable skill and care.

4.2 Paragraph 4.1 shall not apply to the extent of any non-conformance which is caused by use of the Daisy Device Management Service by the Customer or an End User contrary to the Company's instructions, or modification or alteration of the Daisy Device Management Service by any party other than the Company or the Company's duly authorised contractors or agents.

4.3 If the Daisy Device Management Service does not perform in accordance with paragraph 4.1, the Company will, at its expense, use all reasonable but commercially prudent endeavours to correct such failure promptly. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of paragraph 4.1. Notwithstanding the foregoing, the Company:

4.3.1 does not warrant that the Customer's use of the Daisy Device Management Service will be uninterrupted or error-free; or that the Daisy Device Management Service will meet the Customer's requirements; and

4.3.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Daisy Device Management Service may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

4.4 The Company may, at any time, without notice to the Customer:

4.4.1 report to the appropriate authorities any conduct of the Customer or any End User which it believes violates any Relevant Laws;

4.4.2 provide any information the Company has relating to the Customer to any law enforcement or regulatory agency investigating any activity referred to in paragraph 4.4.1 above, or as may be required in relation to legal proceedings concerning the same.

5. Liability

5.1 The performance of the Daisy Device Management Service may be dependent upon the Devices meeting certain minimum system or performance requirements which the Company may notify to the Customer from time to time. Subject to condition 10.5 (Limitation of Liability) of the Mobile Terms and Conditions, the Company shall have no liability to the Customer whether in contract, tort (including without limitation negligence) or otherwise howsoever arising for any performance issues which arise with the Daisy Device Management Service because any Device does not meet any minimum system or performance requirements.

B. Variations to the Mobile Terms and Conditions

1. The following conditions of the Mobile Terms and Conditions shall not apply in respect of the Daisy Device Management Service:

1.1 conditions 5.1, 5.2 and 5.4 (Connection to the System and Provision of the Mobile Network Service);

1.2 conditions 6.6 and 6.7 (Charges and Payment);

1.3 condition 7 (Software); and

1.4 condition 8.1 (Obligations of the Customer).

Schedule 1

Specification

1. Product Overview

The service will be provided with the IBM Endpoint Manager (IEM) software and a number of key components to ensure service infrastructure and software is supported, monitored and maintained. The service is backed up with access to the Daisy Customer Service Desk for resolution of issues and support queries. Daisy will provide customer support via Daisy Customer Service Team. A portal User Guide will also be provided with a Welcome email which provides an overview of the Device Manager Portal and examples as to how to use the software to set up your Security Policy, use the Reports tool and enforce compliance rules.

The software consists of an agent installed on the remote device that connects over the internet to the server. The solution provides a completely integrated approach for managing, securing, and reporting on smart devices. Customer will be provided with secure access to the software that allows your Customer Administrator to set up your Security Policy that will then ensure all your connected devices conform to your requirements.

Key benefits include:

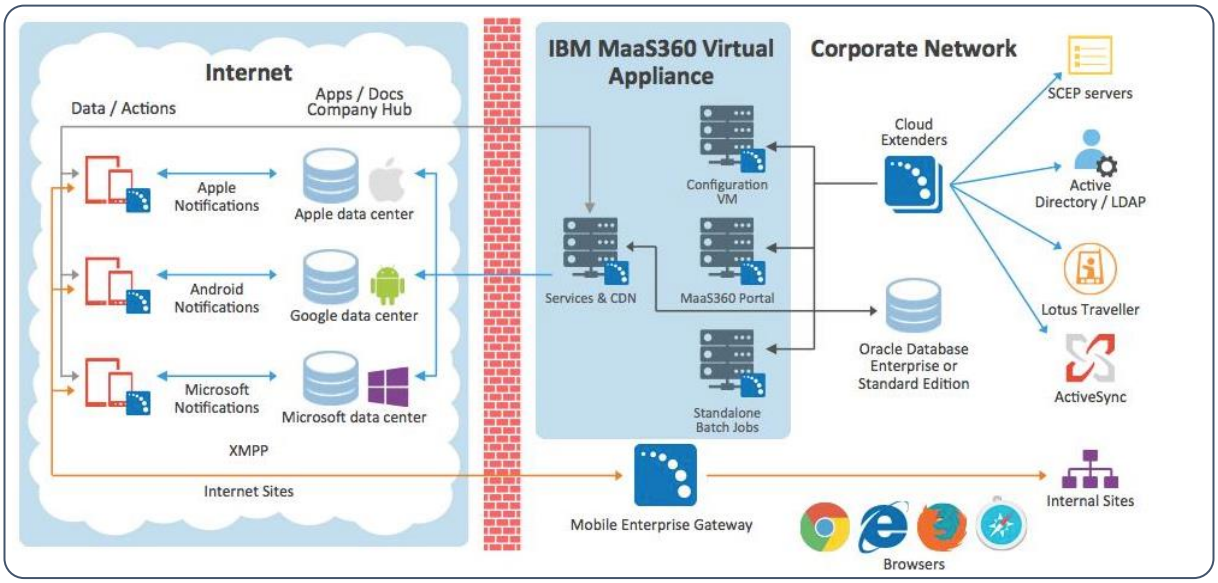
- Remote management of mobile devices 24x7
- Address business and technology issues of security, complexity and bring your own device (BYOD) in mobile environments
- Manage enterprise and personal data separately with capabilities such as selective wipe
- Leverage a single infrastructure to manage all enterprise devices—smartphones, tablets
- Support devices on the Apple iOS and Google Android, Nokia Symbian, Microsoft Windows Mobile.

Each device will require one of the following license types, the license is applied per device for a minimum of 12 months from the time the license was ordered. Should a device be lost or stolen, then this device will need to be reported as lost or stolen by the end user. A license can be removed from a device and applied to an alternative device for the remainder of the contract.

Service Component
Daisy Device Management – Is the fastest and most comprehensive way to configure devices for enterprise access and secure corporate data on smartphones and tablets.
Advanced Daisy Device Management – provides device, application and expense management implemented and controlled through customers corporate policies.
Daisy Secure Productivity Suite - provides secure Email, Browser, Calendar, Contacts, device application and expense management implemented and controlled through customers corporate policies. SPS provides an additional level of security for businesses, locking access to their corporate email, web browser and documents into a special compartment separate to their personal apps and data.

2. Architecture

Daisy Device Manager provides an easy-to-use interface with secure containers provided by IBM. The image to the below shows the products architecture.



IBM (2015) *IBM Knowledge Centre.* Available from: [http://www-01.ibm.com/support/knowledgecenter/SS54PL_2.1.0/com.ibm.maas.doc_2.1/Inst_Guide/Images/ig_architecture.jpg]

3. Service Features

The software consists of an agent installed on the remote device that connects over the internet to a server. Customer Administrators can log into the software to add, change, remove, audit and run reports on their devices.

When teamed together with Secure Productivity Suite our customers can,

- Remotely manage their mobile devices 24x7
- Create a more secure mobile base
- Manage users Business and Personal data separately
- Benefit from only using one infrastructure to manage their mobile devices applications

3.1 Daisy Device Manager

Every organization needs to see and control the mobile devices entering their enterprise, whether they are provided by the company or part of a Bring Your Own Device (BYOD) program. Daisy Device Management (DDM) is the fastest, most comprehensive way to make that happen with;

- Quick and Easy SMS, email, URL enrollment
- Email, calendar, contact profiles configuration
- VPN and Wi-Fi settings configuration
- Device feature configuration
- Security Lock, Wipe and Location Services
- Policy updates & changes
- Inventory management
- Compliance reporting
- Event-based policies
- Proactive expense controls
- BYOD privacy settings
- Self-service portal

3.2 Advanced Daisy Device Manager

Advanced Daisy Device Manager provides a wider range of mobile management and security options across different categories of users, devices, content, and apps, all within the context of their business. This offers the flexibility to implement tiered or layered mobile security to address varied end user needs and IT security requirements.

With Advanced Daisy Device Manager, organisations can phase in BYOD and “right size” their mobile security investments for different classes of users, departments, geographies, devices and applications, and apply the technology approach that best meets the need of those use cases, all from a unified platform.

Includes standard features of Daisy Device Management plus the following;

- **Mobile Application Management**
- Deploy custom enterprise app catalogs
- Blacklist, whitelist & require apps
- Administer app volume purchase programs

- **Mobile Expense Management**
- Monitor mobile data usage with real-time alerts
- Set policies to restrict or limit data & voice roaming
- Review integrated reporting and analytics

3.3 Advanced Daisy Device Manager & Secure Productivity Suite

Advanced Daisy Device Manager & Secure Productivity Suite keeps everything your users need for work in one secure environment with an easy-to-use app launcher. They can manage all their emails, contacts, calendars, enterprise applications and the Web from an isolated workspace on their mobile devices.

With policies to control the movement of data, you can restrict sharing by users, forwarding of attachments, and copying and pasting. Devices that are lost, stolen or compromised can be selectively wiped to remove corporate data.

Through a seamless dual persona style approach, you can put controls in place to manage your data without affecting the rest of the device.

Includes features outlined for Daisy Device Manager and Advanced Daisy Device Manager and includes the following;

- **Secure Mail**
- Contain email text & attachments to prevent data leakage
- Enforce authentication, copy/paste & forwarding restrictions
- FIPS 140-2 compliant, AES-256 bit encryption for data at rest

- **Secure Browser**
- Enable secure access to intranet sites & web apps w/o VPN
- Define URL filters based on categories & whitelisted sites
- Restrict cookies, downloads, copy/paste & print features

- **Application Security**
- Contain enterprise apps with a simple app wrapper or SDK
- Enforce authentication & copy/paste restrictions
- Prevent access from compromised devices

4. Customer User Types

During the ordering process customers will be asked to identify who within their business needs to be set up with the following user types.

User	Function
Customer Administrator (typically an IT Manager)	Maintains direct control over all companies' mobile devices. Is responsible for creating the companies Security Policy using the software provided. Enables full control of where a device is located, secures data 24/7, can push notifications to end user devices for instant communication, provides remote access, has access to all reports and dashboards detailing the current estate.
End User (of the device)	Will be provided with secure access to a personal portal. Can login to report lost or stolen phones - this can be done remotely, online, without the need to contact IT & explain what happened. A report will then be flagged to the Customer Administrator to indicate a devices has been reported as lost or stolen.

4.1 Portal Features for Customers

The Customer Administrator will be provided access to the Maas360 Portal. This is a key part of the service that enables the Customer Administrator to:

- View a central inventory of all devices, software, people and phone numbers
- Manage the relationship of devices to people and phone numbers
- Manage the security of devices remotely including the ability to lock and wipe any device
- Ensure that devices comply to security policy
- Ensure that installed applications comply to corporate policy
- View device properties, optionally including location data
- Run audit reports on actions performed throughout the portal

4.2 Key Benefits

Easy to use online portal – have complete wireless management of your business' devices and because it is hosted on our servers, there is no on-site resources required.

Secure remote wipe facility – preserve your company's data with the ability to wipe devices remotely.

Instant Messaging – with on-screen pop-up messaging customers are able to keep in touch with remote workers without the cost of a text message

GPS location monitoring – keeps track of mobile workers by their devices using the portal's GPS locations feature* this is only available if switched on.

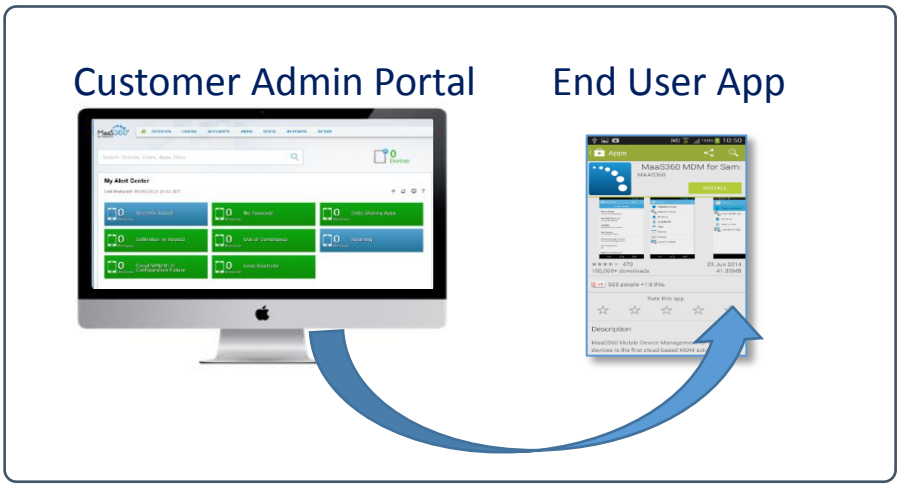
Business reporting – keep abreast of your devices by producing inventory and activity reports.

5. Customer Set Up

Daisy will provide the service as outlined in the below table.

Owner	Customer Service Provisioning Process
Daisy	Send Order Confirmation letter acknowledging the customer order
Customer	Receive Welcome Letter with details as to how to access, login, use the service and contact the Customer Service Team.

The below Diagram shows the software that will be provided to the Customer Administrator and the End User App that will be pushed to the devices identified in the ordering process.



6. Support

The time of the service and the time during which this SLA applies are Monday to Friday 9.00am to 5.00pm. If a subscription is renewed, the version of the SLA that is current at the time that the renewal term commences will apply throughout the renewed term.

6.1 Support Coverage

Online support is available via the chat facility within Daisy Device Management Customer Administrator Portal for all issues relating to Daisy Device Management and Secure Productivity Suite.

All Incidents or Support Queries should be logged with Daisy using the contact details provided in your Order Completion Welcome Letter.

Updates to the software which constitutes the Daisy Device Management Service will be provided where updates are available.

Support does not include assistance for:

a) the design and development of applications;
b) the use of the Daisy Device Management Service other than its specified operating environment; nor
c) failures caused by products for which Daisy is not responsible.

6.2 Incident Priority Definitions

All Incidents and Support Queries shall be responded to by Daisy according to the Target Response Time and resolved within the Target Resolution Time.

The severity codes for all Incidents shall be determined by the customer and Daisy, acting reasonably, using the severity description to agree the code.

On receipt of a notification of an Incident or a Support Query, an initial assessment shall immediately be undertaken by Daisy, a Case Reference Number provided and a Severity Code discussed and promptly agreed with the Customer. Daisy will provide progress updates promptly upon:

- Resolution of the Incident; or
- any change to the Target Resolution Time (which can only occur with the agreement of the Customer)

Daisy shall acknowledge the receipt of all calls or emails that report an Incident or relate to a Support Query to the dedicated Customer Service Team, via email to the designated Customer Administrators including the Case Reference Number.

In the following table, core business hours are defined as Monday to Friday, 9.00 hrs. GMT to 17:00 hrs. GMT.

Severity	Description	Target Response Time	Targeted Status Update Time
PRIORTY 1	An unplanned Incident causing the Software to cease to function.	1 hour	4 hours
PRIORTY 2	Reduced functionality of the Software causing severe disruption. An urgent Support Query.	2 hours	6 hours
PRIORTY 3	Reduced functionality of the Software causing some disruption.	4 hours	12 hours
PRIORTY 4	Non-urgent Support Query. Reduced functionality of the Software resulting in minimal impact.	24 hours	3 Working Days

6.3 Software Availability

The Daisy Device Management and Secure Productivity Suite software has a 99% service uptime. Refer to the Service Level Agreement for further information

Schedule 2

Tariff

	Daisy RRP	MRR or One-Off
Daisy Device Manager	£2.00	MRR
Advanced Daisy Device Manager	£2.40	MRR
Advanced Daisy Device Manager & Secure Productivity Suite	£4.20	MRR