SERVICE DESCRIPTION: MANAGED MOBILITY SERVICES

1. OVERVIEW

1. 1 The Managed Mobility Service permits One New Zealand or our subcontractors to manage and administer the Secure Device Manager on your behalf.

1. 2 When you subscribe to the Managed Mobility Service, you will be licensed to use Secure Device Manager.

1. 3 Secure Device Manager provides remote visibility, tracking, security and control for most smart devices, as well as access to corporate resources and applications. Secure Device Manager consists of a range of Secure Device Manager Services provided through two software applications provided by VMWare INC (the **Third Party Provider**); the Server Software and the Device Software.

1. 4 When we provide you with Managed Mobility Services, you will also receive the Standard Secure Device Manager Services. We will provide you with the Managed Mobility Services and the Standard Secure Device Manager Services in accordance with the terms of:

(a) the Agreement; and

(b) this Service Description.

1. 5 The Third Party Provider will provide you with Secure Device Manager Software, subject to the terms of an End User License Agreement (**EULA**). You must accept the terms of the EULA before activating any Device on the Secure Device Manager Console and/or downloading the Secure Device Manager Software. The EULA will be between you and the Third Party Provider.

1. 6 In the event of any conflict between the terms of:

(a) the Agreement and this Service Description; and

(b) the EULA,

the terms of the Agreement and this Service Description shall take precedence in so far as the conflict arises in relation to the agreement between us and you.

1. 7 By subscribing to the Managed Mobility Services you acknowledge and agree that the Secure Device Manager Console will be managed by One New Zealand Group Limited on your behalf. As a result information collected via the Secure Device Manager Console may also be disclosed to One New Zealand's employees, agents, representatives and third party subcontractors.

1. 8 Unless we agree an alternative solution with you, the Secure Device Manager Console will be hosted by VMWare which means that information collected via the Secure Device Manager Console will be transferred outside of New Zealand, as further described in clause 8.5 below.

2. SOFTWARE

2. 1 You will license the Secure Device Manager Software from the Third Party Provider on a SaaS Licence basis. The term of the SaaS Licence will be governed by the terms of the EULA.

2. 2 You will comply, and ensure your Users comply, with the provisions of the EULA. You acknowledge that the EULA contains certain restrictions around the functionality and use of the Secure Device Manager Software.

2. 3 The Third Party Provider's warranties in respect of the Secure Device Manager Software are set out in the EULA.

2. 4 The Secure Device Manager Software comprises Server Software and Device Software. The Server Software and Device Software will be provided as follows:

(a) the Server Software (other than SEG Software, EIS Software, MAG Software and ACC Software) will be hosted by Vodafone Group Services. Vodafone Group Services will host the Server Software with reasonable skill and care but does not guarantee to provide continuous or uninterrupted access to the Secure Device Manager Services;

(b) if you elect to use the SEG Service, EIS, MAG Service and/or ACC Service, you will be responsible for installing the SEG Software, EIS Software, MAG Software and/or ACC Software (as applicable) on Customer Server Hardware. Such Server Software shall be available for you to download from the Secure Device Manager Console;

(c) the Device Software will be available to the Users via third party application stores. You will ensure that your Users download the official Device Software. Failure by your Users to download the correct Device Software may impact on our ability to provide the Secure Device Manager Services.

2. 5 You will be responsible for ensuring that your Users download the Device Software in a manner which is compatible with the Users' Devices' specific set-up requirements. Users must activate their Devices themselves.

2. 6 Neither we nor the Third Party Provider shall be:

(a) liable to the extent that incorrect downloading of the Device Software has an adverse effect on the operation of Users' Devices; or

(b) responsible for providing any application store through which the Device Software is made available for download to User's Device.

2. 7 You will provide and maintain all necessary hardware, software and the proper environment to operate the Device Software and Server Software installed on Customer Server Hardware as specified in writing by us from time to time, including without limitation acquiring and maintaining the necessary system configuration, hardware, software and licences necessary to utilise the various capabilities of such Software. Neither we nor the Third Party Provider will be responsible for any errors or defects in such hardware or software.

3. MANAGED MOBILITY SERVICES

3. 1 Overview of Managed Mobility Services

(a) When you buy our Managed Mobility Services you may also select our Optional Managed Mobility and Optional Secure Device Manager Services which may incur an additional charge.

(b) We warrant that the Managed Mobility and Secure Device Manager Services will conform in all material respects with the description provided in this Service Description.

(c) You acknowledge that:

(i) we will not provide you with any hardware, including handsets, servers or other infrastructure, as part of the Managed Mobility and Secure Device Manager Services; and

(ii) the Managed Mobility and Secure Device Manager Services do not include the provision of any airtime or data services.

3. 2 Description of Managed Mobility Services

(a) When you set up the Managed Mobility Services you will be required to nominate one or more administrators (Administrator) who may request us to carry out certain tasks on your behalf. You acknowledge that any request we receive from your Administrator will be deemed to have been given with your full authority, including tasks that incur additional costs for your business (Authorised Requests). Any requests for support from your Users which are likely to incur additional costs must be authorised by your Administrator(s).

(b) You will be responsible for communicating set up instructions to your Users.

(c) We will carry out the following tasks on your behalf to set up the Managed Mobility Services:

(i) On-boarding service – On-boarding of a device including set up of Server Software and the installation and configuration of Device Software on the User's devices; and

(ii) Provisioning – Setting up the Users' SIM card/mobile connection according to One New Zealand mobile plan offerings (voice, data and text).

(d) We may carry out the following tasks on your behalf, subject to receiving an Authorised Request from you:

(i) add new Active Devices;

(ii) add and amend policies for Active Devices;

(iii) configure applications and settings on Active Devices;

(iv) lock and wipe Active Devices;

(v) promote, distribute, secure and manage applications on Active Devices;

(vi) email or SMS Users with relevant updates about their Active Device profile or applications; and

(vii) modify reporting for tracking and configuration of Active Devices and for Active Device compliance to corporate policies (such as: password, encryption, and jailbreak detection).

(e) We will carry out the following tasks as part of the Services:

(i) MDM Platform Administration Support;

(ii) Support for Incident Management;

(iii) Support for Change Management;

(iv) Support for Patch Management;

(v) Support for Release Management;

(vi) MDM standard Reporting; and

(vii) Problem Management.

3. 3 Description of Standard Secure Device Manager Services

All customers that select our Managed Mobility Services will also receive the following Standard Secure Device Manager Services:

(a) Standard Secure Device Manager Services will help you to:

(i) support Active Devices with over the air tracking, configuration and policy setting;

(ii) monitor policies for mobile devices and track Active Device compliance to these corporate policies (such as: password, encryption, and jailbreak detection);

(iii) geo-fence policies, applications and documents so they are only available, or their availability is blocked, when the Active Device is within a defined locale;

(iv) remotely view and configure applications and settings on Active Devices;

(v) centrally view Active Devices' inventory and state;

(vi) remotely lock and wipe data from Active Devices;

(vii) promote, distribute, secure and manage applications on Active Devices;

(viii) track telecom service usage; and

(ix) email or SMS Users with relevant updates about their Active Device profile or applications.

Secure Device Manager may be updated by us from time to time with new functionality to support new mobile device operating systems and APIs.

You may need to install third party applications to manage email if your Active Device does not meet minimum device requirements.

(b) On-Boarding Service

The On-Boarding Service provides our standard programme management and implementation services to train your administrator to setup and configure the Server Software in readiness for your activation of the Secure Device Manager Services and enrolment of Devices.

For clarity, the On-Boarding Service does not include consultation on your security policies nor the installation of any Customer Installed Assets, which shall be your sole responsibility.

(c) Support Service

(i) The Support Service includes help desk, incident reporting, management and resolution of incidents, requests to remove, add to, and change user credentials and policy settings, and to add new user credentials and policy settings.

(ii) The Support Service also includes maintenance services (upgrades as well as planned and unplanned server patching) of the Secure Device Manager Console. We may from time to time provide you with updated versions of the Server Software for you to download onto the Customer Server Hardware. You will be responsible for ensuring that your Customer Server Hardware is up to date.

(d) Software Upgrade Access Service

The Software Upgrade and Access Service covers software upgrades of the Secure Device Manager Console and provides you with access to the latest version of the Software when it is made available by us.

Vodafone Group Services manages upgrades of the Secure Device Manager Console.

We will provide updated versions of Server Software for download on Customer Server Hardware via the Secure Device Manager Console. Management and upgrade of the Customer Installed Assets will be performed by you and is your sole responsibility.

3. 4 Description of Optional Services

In addition to the Standard Managed Mobility and Standard Secure Device Manager Services, you can elect to receive one or more of the following Optional Services. Additional charges will apply to the Optional Services. Subject to our rights under the Business Schedule, if we change any of the charges which apply to the Optional Service(s) you have selected, we will give you at least 10 Business Days' notice in writing (including by email) of these changes.

Optional Managed Mobility Services

(a) Professional Services

Professional Services will incur an additional charge as set out in the Pricing Schedule.

Professional Services include the following project management, training and concierge services. We will agree the specific details of any such services you select, in writing:

(i) Project management services include but are not limited to, co-ordinating device staging and deployment, Secure Device Manager profile set-ups and report set-up. Project management services may also include the co-ordination of other Professional Services such as training and the arrangement of concierge services.

(ii) Training services may include one-on-one or group training of end users and 'train the trainer' sessions and the development of bespoke training materials for Managed Mobility.

(iii) Concierge services can be provided on a full or part time basis and can be provided at your sites. Concierge services include supporting any Service related moves, adds, and changes and one on one advice for your staff.

(b) Consultancy Services

Consultancy Services include consulting and Service design services relating to your mobile policy(s) during the initial service implementation phase and will incur an additional charge as set out in the Pricing Schedule.

Consultancy Services can be provided on request to complete a full information and communications technology (ICT) audit. The audit produces a report which catalogues your ICT environment and can be used to inform management of these assets.

Consultancy services can be employed to assist your business on the development of your mobility strategy and mobile device management policies.

4. RESTRICTIONS ON USE OF THE SECURE DEVICE MANAGER SERVICES AND SOFTWARE:

4. 1 You will not use, and will not authorise or permit any third party including any User to use, the Secure Device Manager Services and/or Software:

(a) on any device which is not an Active Device; and/or

(b) on any Device which is not connected to our network except where you are roaming outside New Zealand or you have other Devices which are connected to an overseas network, as agreed on a case by case basis; and /or

(c) in an Embargoed Territory.

4. 2 We will be under no obligation to provide any of the Secure Device Manager Services in the event of any incidents caused by or related to the following:

(a) the failure of any system or code, or use of any software or hardware used by you in connection with the Secure Device Manager Services which has not been approved, authorised or supplied by us;

(b) any incident which we are unable to verify or reproduce after making commercially reasonable efforts;

(c) any incident which could have been prevented by you running the most up-to-date release and version of the Software (including any fixes or patches) made available by us or the Third Party Provider; and/or

(d) any incident or problems caused by, or contributed to by, your negligence, abuse, misuse and/or misapplication of the Software or any failure by you to comply with the terms of this Agreement.

5. CUSTOMER INSTALLED ASSETS (ON CUSTOMER SERVER HARDWARE)

5. 1 The SEG Service, EIS, MAG Service and ACC Service require Customer Server Hardware. If you elect to use the SEG Service, EIS, MAG Service and/or ACC Service, you will be responsible for:

(a) installing the SEG Software, EIS Software, MAG Software and/or ACC Software (as applicable) on the Customer Server Hardware and for implementing any updates and new releases to such Server Software;

(b) providing, operating and maintaining the Customer Server Hardware, including security of the Customer Server Hardware;

(c) ensuring that the Customer Server Hardware meets the minimum technical requirements as advised by us from time to time; and

(d) ensuring that you have entered into the EULA and are licensed to use the Server Software.

6. ONE NEW ZEALAND STORAGE EQUIPMENT:

6. 1 You will be entitled to use the One New Zealand Storage Equipment, provided that you comply with the following provisions of this clause 6.

6. 2 Where you store any content on the One New Zealand Storage Equipment, you will ensure that the content does not infringe any applicable laws, regulations or third party rights (such as material which is obscene, indecent, pornographic, seditious, offensive, defamatory, threatening, liable to incite racial hatred, menacing, blasphemous or in breach of any third party Intellectual Property Rights or rights under the Privacy Act 2020) (**Inappropriate Content**).

6. 3 You acknowledge that we have no control over any content placed on the One New Zealand Storage Equipment by you or your Users and we do not purport to monitor the One New Zealand Storage Equipment. We reserve the right to remove content from the One New Zealand Storage Equipment where we reasonably suspect such content is Inappropriate Content. We will notify you if we become aware of any allegation that content on the One New Zealand Storage Equipment may be Inappropriate Content.

6. 4 You will indemnify us against all damages, losses, costs and expenses arising as a result of any action or claim that the content or any other material stored on the One New Zealand Storage Equipment constitutes Inappropriate Content.

7. PROTECTION OF USER NAMES AND PASSWORDS

7. 1 We will provide a Secure Device Manager administrator (as agreed with you) with a user name and password at the time of set-up. You will ensure that such details are kept secure, and used only in accordance with the Agreement.

8. DATA PROTECTION AND PRIVACY

8. 1 You acknowledge and agree that:

(a) User Personal Information is collected and processed as a result of the Services being provided; and

(b) for the purposes of the Privacy Act 2020 and any other applicable data protection legislation, you are the agency that is collecting User Personal Information and we only hold such User Personal Information on behalf of you and not for our own purposes.

8. 2 You will be responsible for compliance with the principles set out in the Privacy Act 2020 and any other applicable data protection legislation, including without limitation:

(a) notifying Users and obtaining their consent to their Personal Information (including urls visited by Users via their Active Devices) being collected by you and disclosed to us and our sub-contractors and/or related entities in connection with the provision of the Secure Device Manager Services by us;

(b) if you opt to use location-based services, ensuring that you have all necessary consents from each User to allow us to provide you with geographical tracking information about such User;

(c) determining how to manage and secure the Active Devices using the Software and the Services;

(d) determining the Users' rights to access mobile content, corporate services and mobile applications on the Active Devices; and

(e) maintaining the primary location group and group ID and ensuring that the master location group enabled by us is not amended at any time,

in each case in advance of activating a Device or Service or requesting us to provide any User information to you.

8. 3 The EULA contains separate data protection provisions in respect of processing of User Personal Information carried out by the Third Party Provider in connection with its provision of the Software to you. The Third Party Provider shall be directly responsible to you for any processing of User Personal Information pursuant to the data protection provisions set out in the EULA.

8. 4 You acknowledge and authorise the use of anonymous transaction data to create aggregated, statistical data and information about service usage and devices that does not, and cannot be used to, identify a User.

8. 5 You acknowledge and agree that the Secure Device Manager Console is hosted and managed by VMware inc. Accordingly, information collected via the Secure Device Manager Console may be disclosed to VMware (including its employees, agents and representatives) and transferred to, and stored in, jurisdictions outside New Zealand. In particular:

(a) in general, information collected via the Secure Device Manager Console is transferred to, and stored on servers managed by, VMWare inc in Australia;

(b) in order to provide the Support Services, information collected via the Secure Device Manager Console may be accessed by representatives of the One New Zealand Service Desk (which is managed by One New Zealand); and

(c) in order for you to use certain Secure Device Manager Services, specific information collected via the Secure Device Manager Console may be transferred to, and stored on, servers in other jurisdictions outside New Zealand. For example, 'auto-discovery' is an optional Secure Device Manager feature which allows your end-users a faster way to enrol their Device onto Secure Device Manager. If you select the auto-discovery service, in order for your end-users to use the service, your corporate email domain, the hashed MAC address of the enrolling Device, your Secure Device Manager Group ID and the Secure Device Manager Server URL (https://mdm.vodafone.co.nz) will be transferred to and stored on the Third Party Provider's (or an associated company of the Third Party Provider's) auto-discovery server hosted in Australia.

9. LIABILITY

9. 1 In addition to the liability exclusion and limitation provisions of the Business Terms, we will not be liable under this Service Description whether in contract, tort (including negligence), breach of statutory duty, indemnity or otherwise for any loss, whether direct or indirect:

(a) suffered by you in connection with the Software and you will bring all claims for any losses suffered in connection with the Software against the Third Party Provider pursuant to terms of the EULA;

(b) which results from the combination of a Service with hardware, software or other materials which are not essential for the conventional performance of the Service and/or are not otherwise provided, recommended or authorised by us, where absent such combination the Service would not be the subject of the infringement claim; or

(c) suffered by you as a result of us performing a task in accordance with your Authorised Request, except to the extent our performance amounts to a breach by us of our obligations under this Service Description.

9. 2 We exclude all liability in the event we are unable to provide the Managed Mobility and Secure Device Manager Services for Apple® devices due to you failing to have your own APNS Certificate and your own relationship with Apple's iOS Developer Enterprise Program or its Volume Purchase Program.

10. TERM AND TERMINATION

10. 1 **Term**: This Service shall start on the date that you activate Secure Device Manager and continue until terminated in accordance with the remainder of this clause 10 and/or the Agreement (Term).

10. 2 **For Convenience**: In addition to the termination rights set out in the Agreement, either party may end this Service on thirty (30) days prior written notice to the other.

10. 3 In the event you terminate the Services under clause 10.2, we won't charge you for Services for the month your notice takes effect. Charges for the previous billing cycle will still be payable

10. 4 **For termination of the EULA**: We may terminate this Service immediately upon written notice to you if the Third Party Provider or you terminate the SaaS Licence for the Software.

11. RIGHTS FOLLOWING TERMINATION OF THIS SERVICE AND/OR THE AGREEMENT

11. 1 Upon termination of this Service and/or the Agreement:

(a) the provisions of the EULA relating to Term and Termination shall apply in respect of the Software;

(b) we will cease our provision of the Services from the effective date of termination;

(c) we will cease your access to the Secure Device Manager Console from the effective date of termination; and

(d) to the extent we hold any User Personal Information, we may retain such User Personal Information to the extent required to by the Privacy Act 2020 or other applicable data protection legislation.

12. DEFINITIONS

In this Service Description capitalised words shall have the same meanings as in the Agreement save as set out below:

Active Device means a Device which has been registered on the Server Software by you or on your behalf to receive the Secure Device Manager Services;

Authorised Request means a request received from an Administrator as further described in clause 3.2.

Customer Installed Assets means the ACC Service, MAG Service, EIS and/or SEG Service (as applicable) installed on your Customer Server Hardware;

Customer Server Hardware means a Customer-managed server on your premise on which the ACC Service, MAG Service, EIS and/or SEG Service (as applicable) is installed;

Device means a mobile device which is capable of receiving the Secure Device Manager Services;

Device Software means the official equipment software for Users' Active Devices (including any new versions or releases of the same) provided by the Third Party Provider to facilitate the provision of the Secure Device Manager Services including (without limitation), if selected by you:

(a) the Secure Browser Software; and

(b) the Secure Content Locker Software;

Embargoed Territories means Cuba, Iran, North Korea, Sudan and Syria and any other territory which is, or during the Term becomes, subject to export restrictions and/or sanctions imposed by either the United Kingdom or the United States of America;

EULA means the SaaS Licence EULA between you and the Third Party Provider for the provision of Software on a subscription licence basis;

Inappropriate Content has the meaning set out in clause 6.2 of this Service Description;

Managed Mobility Services mean the services described in clause 3 of this Service Description;

On-Boarding Service mean the on-boarding service as further described in clause 3.3 of this Service Description;

Optional Managed Mobility Services means the services described in clause 3.4 of this Service Description;

SaaS Licence means a subscription licence to the Software, as further described in the EULA;

Server Software means the Server Software provided by the Third Party Provider (including any new versions or releases of the same) to facilitate the provision of the Secure Device Manager Services, including (without limitation) if selected by you:

(c) ACC Software;

(d) BIS Software;

(e) EIS Software;

(f) MAG Software;

(g) SEG Software; and

(h) Secure Device Manager Software;

Software means, collectively, the Device Software and Server Software provided by the Third Party Provider to facilitate the provision of the Secure Device Manager Services;

Standard Secure Device Manager Services means the standard services provided by us via the Secure Device Manager Console from time to time, including without limitation, the following services (as further described in clause 3.3 of this Service Description):

(i) Secure Device Manager;

(j) On-Boarding Service;

(k) Support Service; and

(l) Software Upgrade Access Service;

Support Service means the support service as further described in clause 3.3 of this Service Description;

Third Party Provider means VMware Inc (whose headquarters are at 3401 Hillview ave, Palo Alto, California, USA) or such other third party provider as may be identified in the EULA from time to time;

User means an end-user of an Active Device;

User Personal Information means personal information (as defined in the Privacy Act 2020 or any similar term as defined in any other applicable data protection legislation) about a User;

One New Zealand Storage Equipment means the equipment made available by us to you for the storage of your content;

Secure Device Manager means our secure device manager service as further described in this Schedule;

Secure Device Manager Console means the interface used by your administrator to access Secure Device Manager Services;

Secure Device Manager Services means the Optional Secure Device Manager Services and Standard Secure Device Manager Services provided by us via the Secure Device Manager Console from time to time; and

Secure Device Manager Software means the Server Software provided by the Third Party Provider (including any new versions or releases of the same) to us during the Term to facilitate the provision of the Secure Device Manager Console.