Part K – Enterprise Mobility Management

Contents

1	**About this Part**	**2**
2	**Enterprise Mobility Managed Service 3**	**2**
3	**Enterprise Mobility Managed Service 2**	**16**
4	**Enterprise Mobility Managed Service**	**54**
5	**Telstra Mobile Device Management ("T-MDM") service**	**99**
6	**Mobile Workspace**	**126**

Part K – Enterprise Mobility Management

Certain words are used with the specific meanings set out in Part A – General of the Telstra Mobile section, or in the General Terms of Our Customer Terms.

1 About this Part

1.1 This is part of the Telstra Mobile section of Our Customer Terms. Provisions in other parts of the Telstra Mobile section, as well as in the General Terms of Our Customer Terms, may apply.

See clause 1 of the General Terms of Our Customer Terms for more detail on how the various sections of Our Customer Terms should be read together.

2 Enterprise Mobility Managed Service 3

What is the Enterprise Mobility Managed Service 3 (EMMS 3)?

2.1 Enterprise Mobility Managed Service 3 (**EMMS 3**) is an end-to-end managed service to support your mobile ecosystem, encompassing consulting, design and implementation, management of your mobile threat detection and mobile device management platforms, service desk and end user support services, and business intelligence capabilities.

2.2 EMMS 3 is available in the following service tiers:

(a) **EMMS 3 Foundation:** provides management of devices on your cloud infrastructure as described in this clause 2; and

(b) **EMMS 3 Advanced:** provides management of your devices, applications and content on your hybrid on premise and cloud infrastructure as described in this clause 2.

2.3 Unless otherwise expressed, the terms and conditions outlined in this clause 2 apply to both EMMS 3 Foundation and EMMS 3 Advanced.

Eligibility

2.4 EMMS 3 is not available to Telstra Wholesale customers or for resale. You must not re-supply EMMS 3 services to a third party.

2.5 EMMS 3 Foundation is only compatible with the mobile device management ("**MDM**") platform (VMWare Workspace ONE Standard) provided as part of the EMMS 3 service

("**MDM Platform**"). Your MDM Platform supports mobile device management.

2.6 EMMS 3 Advanced is only compatible with the enterprise mobility management ("**EMM**") platform (VMWare Workspace ONE Advanced) provided as part of the EMMS 3 service ("**EMM Platform**"). Your EMM Platform includes the MDM Platform functionality and also supports mobile content and mobile application management.

2.7 You cannot consume EMMS 3 Foundation and EMMS 3 Advanced on the same account.

Features

2.8 The following table reflects the key inclusions of your relevant EMMS 3 service, with the more detailed features described further below

Service Feature	Description	Included	
		EMMS 3 Foundation	EMMS 3 Advanced
End-to-end management of your MDM Platform and MTD Platforms	We will setup and configure your MDM Platform and MTD Platforms, including integrating the MTD Platform and your Active Directory implementation (if any) with the MDM Platform. We will maintain your MDM and MTD Platforms on an ongoing basis, including deploying updates in a timely manner, and implementing your policies agreed in the CSEM on and through these platforms to your end users Registered Devices.	Y	Y
The end-to-end management of your EMM Platform	We will set up and configure your EMM Platform and assist with the integration of the EMM Platform into your on premise and cloud infrastructure.	N	Y
End User Support	We will provide a help desk available by phone and email, and will support your End Users to agreed service levels.	Y	Y
Visibility of organisation wide tickets	For those organisations that want to keep visibility of incident, service request and change request tickets, Telstra can provide an integration mechanism between Telstra's IT service management system and your IT service management system, subject to compatibility.	Y	Y

Business Reporting Insights	**EMMS 3 Foundation** We will provide your nominated admin user with access to pre-configured core reports, with information about how your business consumes the managed service, service desk utilisation on incidents & requests, change management, licence, mobile threat, operating system and fleet reports. **EMMS 3 Advanced** We will provide your nominated admin user with access to pre-configured core reports, with information about how your business consumes the managed service, service desk utilisation on incidents & requests, change management, licence, mobile threat, operating system and fleet reports.	Y	Y
MDM or EMM platform and licensing – VMWare Workspace ONE	**EMMS 3 Foundation** EMMS 3 Foundation includes VMWare Workspace ONE Standard licensing for each Registered Device. **EMMS 3 Advanced** EMMS 3 Advanced includes VMWare Workspace ONE Advanced licensing for each Registered Device. As part of EMMS 3, we will provide a Telstra dedicated environment used for shared multiple / multi-tenant customers.	Y	Y
Mobile Threat Detection (MTD) platform and licensing – Zimperium	EMMS 3 includes Zimperium zConsole platform license, and zIPS app licensing for each Registered Device. As part of EMMS 3, we will provide a Telstra dedicated environment used for shared multiple / multi-tenant customers, and integrated with your MDM or EMM platform (as applicable), with on-device endpoint protection deployed to your end user's Registered Devices.	Y	Y

2.9 You may choose to extend EMMS 3 with one or more of the following Optional Services:

Optional Service	Description	Available

Part K – Enterprise Mobility Management

Feature		EMMS 3 Foundation	EMMS 3 Advanced
24x7 End User Support	If you take up optional 24x7 End User Support, we will extend the End User Support to provide 24x7 support as further described below.	Y	Y
Mobility Service Manager	If you take up the option of a Mobility Service Manager, we will enhance your EMMS 3 managed service with proactive consulting and collaboration further described below.	Y	Y
Fleet Management	If you take up optional Fleet Management, we will also provide device procurement and logistics, device staging, allocation and deployment, management of device repairs and replacements, and fleet location management as part of your EMMS 3 service.	Y	Y
Professional Services	Any further or additional professional services agreed in a Statement of Work on the terms set out in the Professional Services section of Our Customer Terms.	Y	Y
Mobile Usage Management (MUM)	If you take up the optional Mobile Usage Management (MUM) service, we will enhance your EMMS 3 Advanced service with data and content management capability as further described below.	N	Y

2.10 We will provide the initial planning, implementation and transition services, and any further professional services agreed in a Statement of Work on the terms set out in the Professional Services section of Our Customer Terms.

2.11 From time-to-time, we may need to implement planned outages to your MDM or EMM Platform (as applicable), your MTD platform, and if applicable, your MUM Platform for maintenance and upgrade purposes. We will provide you with prior reasonable notice before commencing any transfer or planned outages and will aim to cause as little impact as possible to your EMMS 3 service when we do.

2.12 We may require you or your End Users to agree to a further end user licence agreement (EULA) with us (or our third party suppliers) to access the MDM or EMM Platform (as applicable), your MTD platform, and if applicable, your MUM Platform (and/or MUM dashboard and End User application) and to install the endpoint protection application on their Registered Device.

2.13 We do not represent that EMMS 3 (including MDM or EMM Platform (as applicable), MTD platform, and if applicable, your MUM Platform) integrate with any third party software or service unless expressly set out in your agreement with us.

Customer Services Engagement Manual

2.14 As part of the implementation services, we will work with you to create and agree upon a Customer Services Engagement Manual (**CSEM**), documenting the roles, responsibilities, and agreed processes that we will follow to deliver your EMMS 3 service.

2.15 The CSEM is the single point of reference for both parties on the operational aspects of your EMMS 3 service. Changes to the CSEM require mutual agreement. You may request changes at any time through the change management process documented in the CSEM. Changes to the CSEM may incur additional cost.

2.16 We may, but are not required to, act on instructions of your authorised administrators (other than changes to authentication processes) that are inconsistent with the processes documented and agreed in the CSEM.

Third Party Suppliers

2.17 Some aspects of your EMMS 3 service may be the responsibility of a third party or conditional upon action by a third party. To the extent the CSEM defines an action as a third party responsibility:

(a) we are not responsible for any delay or inaction by the third party; and

(b) as between you and Telstra, each responsibility of the third party is deemed to be your responsibility.

2.18 To avoid doubt, third party suppliers in clause 2.17 do not include Telstra's related entities such as BTS Mobility, or licensors of Telstra provided MDM or EMM (as applicable), , MTD, and if applicable, MUM capabilities.

2.19 You appoint us as your agent to act on your behalf in relation to any third party supplier to the extent specified in the CSEM, including entering purchase agreements on your behalf.

2.20 You authorise us to provide your contact details and all other necessary information (including confidential information) to any third party suppliers, and to instruct third party suppliers on your behalf, to the extent necessary for us to provide EMMS 3. Upon request, you must provide all assistance we reasonably require to provide EMMS 3, including authorisations to third party suppliers.

End Users and Supported Devices

2.21 We will only provide EMMS 3 in respect of your End Users we have authenticated in accordance with the processes agreed in the CSEM, who are using a device that meets the requirements of clauses 2.22, 2.23, 2.24 or as otherwise specified in your agreement with us (**Supported Device**).

2.22 EMMS 3 will only support devices that are:

(a) connected to a Telstra mobile or mobile data plan; or

(b) connected to a mobile or mobile data plan from a carrier other than Telstra; or

(c) connected to the internet using Wi-Fi only.

2.23 EMMS 3 will only support devices using the following operating system versions:

(a) iOS 10.0 and above;

(b) Windows 10 Phone, also known as Windows 10 Mobile and above (to avoid doubt, this does not include Windows 10 S operating system compatible with some 2-in-1 and tablet devices);

(c) Android 6.0 and above.

2.24 EMMS 3 capabilities, other than enrolment and unenrolment support, will only be available to your end users who have enrolled their Supported Device on the MDM Platform or EMM Platform (as applicable) (**Registered Devices**), and that device is turned on and connected to the internet.

Managed Service for MDM and MTD

2.25 We will procure, provision, and manage the Zimperium and the relevant VMWare Workspace One software licenses. We will provide the MDM or EMM Platform (as applicable) and MTD platform as a Telstra dedicated environment used for shared multiple / multi-tenant customers.

2.26 We will provide the following capabilities as part of your EMMS 3 Foundation (MDM) or EMMS 3 Advanced (EMM) managed service:

Category	Description	Included	
		Foundation	Advanced

Part K – Enterprise Mobility Management

Deploy	Deploy VPN Profile to Registered Devices	Y	Y
	Deploy up to 5 public apps and 1 in-house app to Registered Devices	Y	Y
	Deploy and configure managed apps to enable app protection polices	N	Y
	Deploy Wi-Fi, restrictions, VPN, email, web clip and policy / security server configurations to Registered Devices	Y	Y
	Deploy, install and record instance and approved licenses to Registered Devices	Y	Y
	Deploy configuration for connecting to online content repositories, intranet access, secure groups and publish to user groups.	N	Y
	Deploy certificate based multi factor authentication.	N	Y
	Deploy additional or modified EMM profiles and compliance actions agreed with you.	N	Y
	Deploy MTD app devices enrolled in customers MDM or EMM Platform (as applicable).	Y	Y
Assist	Enrolment and un-enrolment end user support	Y	Y
	MDM or EMM (as applicable) agent app end user support	Y	Y
	Device configuration end user support	Y	Y
	Lost and stolen device end user support	Y	Y
	MDM and EMM Platform (as applicable) connectivity support	Y	Y
	Managed app and corporate content connectivity and access support	N	Y
Manage	Maintenance of the MDM or EMM Platform (as applicable), including timely deployment of updates.	Y	Y

Part K – Enterprise Mobility Management

	Maintenance of the EMM Platform for the following on premises components (excluding identity): • email / exchange on premise connector • platform or cloud certificate connector install and configurations of connectors. We will not maintain your virtual hardware, operating system or network.	N	Y
	Updates to enrolment documents.	Y	Y
	Apple Push Notification Service (APNS) certificate renewal	Y	Y
	Maintenance of user or device certificates	Y	Y
	Profile and policy changes	Y	Y
	Changes to your VPN profile upon request.	Y	Y
	Administrator role management	Y	Y
	Compliance rules and enforcement actions management	Y	Y
	Change management assistance	Y	Y
	Corporate app store updates to add or remove manages apps	N	Y
	Content repository access updated	N	Y
	Conditional access policy updates	N	Y
	Single Sign On (SSO) application configuration updates	N	Y
	Manage and enforce Registered Devices to be encrypted	Y	Y

2.27 We will provide the below capabilities as part of your MTD managed service. These capabilities are applicable for both EMMS 3 Foundation and EMMS 3 Advanced.

Category	**Description**
Deploy	Deploy Zimperium zIPS app to Registered Devices

Assist	Threat detection and end user support
	Enrolment and un-enrolment end user support
	Agent app and notifications end user support
	Mobile Threat Detection platform connectivity support
Manage	Maintenance of the MTD platform (zConsole), including timely deployment of updates.
	Threat detection
Control	Ongoing detection of device, network and application threats
	Threat remediation in accordance with CSEM defined process.
	Threat response platform policy updates

2.28 Threat remediation provided with EMMS 3 is limited to MDM or EMM Platform and MTD platform capabilities. Some remediation actions may cause business interruption or loss of data, for example deleting an application, deactivating device connectivity, or removal of corporate data from the device. You accept responsibility for any such interruption or loss caused by our implementation of remediation actions as defined in the CSEM.

Optional Mobility Service Manager Add-on

2.29 If you take up the optional Mobility Service Manager service, we will provide a service manager who will provide the below enhanced capabilities as part of EMMS 3. These capabilities are applicable for both EMMS 3 Foundation and EMMS 3 Advanced.

Category	Description
Informing	Monthly solution and service reporting Release information regarding mobile OS updates Access to mobility experts and leaders who are involved in mobile strategy across multiple organisations Managing of mobile OS updates and alignment / validation to business use-cases Advice around events in the ubiquitous world of enterprise mobility

Planning	Device OS roadmap & strategic planning Fleet Lifecycle Management planning Participation in mobile strategy discussions Keeping Customer Solution Documentation up to date Release Management roadmap management Aligning customer solution to industry best practise
Enhancements	Service enhancements to leverage new device and platform capabilities Compliance rules and actions (MDM or EMM configuration as applicable) Protective Maintenance and Routine Health Checks Development and ongoing management of Customer use-case test plans for OS and platform release updates Releases analysed against each of the customers use cases to ensure operational excellence Providing access to industry experts and partners.

Optional Fleet Management Add-on

2.30 If you take up the optional Fleet Management capability, we will provide the below enhanced capabilities as part of EMMS 3. These capabilities are applicable for both EMMS 3 Foundation and EMMS 3 Advanced.

Category	Description
Device procurement & reverse logistics	Management of device ordering, fulfilment and any logistics in relation to device ordering
Device staging, allocation and deployment	Management of the device staging and MDM or EMM enrolment processes (as applicable) prior to delivering to the end user
Device repair and replacement management	Management of device hardware faults, repair processes, and a device spare pool for device replacements
Fleet Location Management and Tracking	Management of device to user assignments and locations of devices

Asset Reports	New device orders per month Devices deployed per month Devices repaired per month Asset allocation per month

End User Support – Service Desk Availability

2.31 For both the EMMS 3 Foundation and EMMS 3 Advanced, we will provide end user support through the Service Desk to the Service Levels specified below. Unless otherwise agreed, the Service Desk is available Monday to Friday 8am to 8pm AEDT, excluding public holidays in Sydney, Australia.

2.32 Despite clause 2.31, the Service Desk is available 24x7 for the following requests (optional 24x7 End User Support is not required for these capabilities):

(a) Reporting and remediation of severity 1 incidents;

(b) Lost & stolen device support: end user support for lost or stolen devices – lock device, remove corporate data and access, locate device, reset to factory settings;

(c) Password reset / unlock device;

(d) Roaming: incident support for users travelling overseas

2.33 For both the EMMS 3 Foundation and EMMS 3 Advanced, if you take up Optional 24x7 End User Support, we will provide extended 24x7 Service Desk availability for all incidents and requests, excluding the following:

(a) change approval activities;

(b) change management;

(c) fleet services that rely on logistics; and

(d) any third-party provided service (including the MDM or EMM Platform, the MTD Platform and if applicable, the MUM service) that is available:

(i) only during business hours; or

(ii) as agreed in the CSEM.

Optional Mobile Usage Management Add-on

2.34 If you take up the optional Mobile Usage Management ("**MUM**") service, we will provide the enhanced capabilities outlined in the table below. The MUM service is only available as an optional add on to EMMS 3 Advanced (and not for EMMS 3 Foundation).

Category	Description
Data compliance management	Manage content filtering based on content category and type Manage data pool consumption Manage restrictions on unapproved usage Manage alerts and enforce data caps (domestic, roaming, and Wi-Fi)
Policy enforcement	Visibility of mobile data type (e.g. http, https, application data) Manage notifications for authorised representatives and end users Manage compression of videos and images Manage user access to domains and URLs Manage downloads from unofficial, unauthorised or untrusted app stores Manage data usage profile and policy updates
Management of integrated platforms	We will manage the integration between the MUM Platform and the supported EMM platform under Telstra Mobility Managed Service Advanced, in terms of additional or modified EMM profiles and compliance actions that are supported for the data usage management solution.
End user support	End user support provided as part of your EMMS 3 Advanced service will be extended to the MUM service. Wandera app end user support: assistance and enquiries. Assistance for authorised customer administrative staff who seek reporting and mobile data policy changes. Access and connectivity to corporate infrastructure support. Wandera and EMM app notifications end user support

Reporting	Reporting through MUM dashboard on how data is being used (app and website usage) across the fleet of devices and customised down to individual device and application. This reporting is for a service owner or administrator. Reporting insight for an end user into how data is used (app and website usage), through an End User app on Registered Devices.

2.35 The MUM service is only compatible with the MUM Platform (Wandera Limited platform), and we will provide you with access to an End User app on Registered Devices. We will also provide up to 5 authorised users with read only access to an MUM dashboard for reporting purposes.

2.36 The MUM service will support cellular and WiFi coverage.

2.37 The MUM service will support the following browser versions:

(a) Mozilla Firefox 38 or above;

(b) Google Chrome 56 or above;

(c) Apple Safari 9 or above;

(d) Microsoft Edge 12 or above; and

(e) Microsoft Internet Explorer 11.

2.38 Notwithstanding the Supported Devices described at clause 2.21, in relation to unsupervised iOS devices, the MUM service will support devices with an operating system version of iOS 10.2 and above.

Service Levels

2.39 We will provide EMMS 3 to the following service levels, or as otherwise specified in your agreement with us. We will use reasonable commercial efforts to meet the target response, communication frequency, resolution time:

INCIDENT SEVERITY	TARGET RESPONSE TIMES	TARGET COMMUNICATION FREQUENCY	TARGET RESTORATION TIMES	SERVICE LEVEL TARGET
1 (CRITICAL)	15 min	1 hours	4 hours	90%
2 (MAJOR)	30 min	2 hours	8 hours	90%
3 (MINOR)	1 hour	8 hours	1 business day	90%

4 (URGENT REQUEST)	2 hours	12 Hours	3 business days	90%
5 (STANDARD REQUEST)	3 hours	24 Hours	5 business days	90%

Severity 1 (Critical) means failure of the system with a major business impact affecting more than one End User, business critical system or process with no workaround.

Severity 2 (Major) means one or more End Users are affected by the failure of a business critical system which may have a workaround that cannot be sustained over a reasonable period of time (more than 1 day).

Severity 3 (Minor) means one End User is affected and not business critical which may have a workaround that can be sustained over a reasonable period of time (more than 1 day).

Urgent Request means a service request for one or more End Users, which has some urgency owing to business requirements or targets.

Standard Request means a service request for one or more End Users, which has no immediate impact and the request is not business critical.

2.40 Service Level targets above:

(a) operate during the Service Desk availability times described in clauses 2.32, 2.32 and 2.33 above; and

(b) will not apply in relation to any period of scheduled maintenance; and

(c) are targets only, you acknowledge and agree that, unless otherwise agreed in your separate agreement with us, we are not liable to you for any failure to meet the service level targets.

2.41 We will not be responsible for a failure to meet a service target to the extent that such failure is caused by your delay in actioning items that are your responsibility, a third party responsibility (as agreed in the CSEM), or that are caused by your breach of this agreement.

2.42 The service level targets (and incident descriptions) do not apply to the optional MUM service, and the service level targets (and incident descriptions) applicable to the optional

MUM service will be as agreed in the CSEM.

Charges

2.43 The charges for EMMS 3 are set out in your agreement with us.

Minimum Commitment and Early Termination Charges

2.44 EMMS 3 has a minimum term of 12 months.

2.45 You may be required to pay us an early termination charge if, before the end of the minimum term:

(a) you cancel your EMMS 3 service (when we are not in breach); or

(b) we cancel your EMMS 3 service because you are in breach of your agreement with us.

2.46 The early termination charge is set out in your agreement with us.

3 Enterprise Mobility Managed Service 2

Enterprise Mobility Managed Service 2 is only available to customers who sign a new Enterprise Mobility Managed Service 2 agreement on and from 1 February 2014, unless otherwise agreed).

What is the Enterprise Mobility Managed Service 2?

3.1 Our Enterprise Mobility Managed Service 2 provides Supported EMP Applications which we will monitor, manage, maintain and provide user support services for, by way of a managed application layer for eligible customers in relation to Enterprise Mobility services and Supported Devices.

What is the Enterprise Mobility Platform?

3.2 The Enterprise Mobility Platform ("**EMP**") is the component of the Enterprise Mobility Managed Service 2 that provides device management services to Supported Devices, or manages the Supported EMP Applications and the corporate wireless data synchronisation. The EMP consists of server infrastructure, an operating system and a Supported EMP Application. You may also purchase Additional Services as set out in these terms.

3.3 For an Enterprise Mobility Managed Service 2 to support Supported Devices (other than BlackBerry devices), you must connect the Supported Devices to an EMP. The EMP can either be hosted by us or by a Supported EMP Vendor (to ensure the Supported EMP Vendor's EMP is compatible with your Enterprise Mobility Managed Service 2).

3.4 If the EMP is hosted by us or a Supported EMP Vendor, certain terms below regarding the Enterprise Mobility Managed Service 2 will not apply to you (as specified below).

3.5 To use the Enterprise Mobility Managed Service 2, you may be required to agree to an End User Licence Agreement ("**EULA**") in relation to the Enterprise Mobility Managed Service 2 with a Supported EMP Vendor or other third party supplier approved by us. We can provide a copy of the EULA to you upon request.

Supported Devices

3.6 The Enterprise Mobility Managed Service 2 will only support Supported Devices which are:

(a) connected to a Telstra mobile data plan ("**Telstra Supported Device**"); and

(b) connected to a mobile data plan from a carrier other than Telstra or is Wi-Fi only ("**BYO Supported Device**").

Minimum Term

3.7 Unless we otherwise agree, there is no minimum term for Enterprise Mobility Managed Service 2. It is offered as a casual month to month service.

Service charges

3.8 You must pay us the Enterprise Mobility Managed Service 2 charges specified below. For the avoidance of doubt, these service charges do not include any charges for any telecommunications services used in connection with the Enterprise Mobility Managed Service 2.

Monthly Support charges (Telstra Supported Devices)

3.9 We will charge you the following monthly support charge for each Telstra Supported Device:

Service component	Monthly charge per Supported Device (ex GST)	Monthly charge per Supported Device (incl. GST)

Service Desk support (per Supported Device)	$9.09	$10.00

3.10 Depending on what Enterprise Mobility Managed Service 2 tier you choose, we may also charge you the following monthly support charge for each Telstra Supported Device:

Service component	Monthly charge per Supported Device (ex GST)	Monthly charge per Supported Device (incl. GST)
Tier 1 – Supported EMP Applications	$6.00	$6.60
Tier 2 – Supported EMP Applications	$13.64	$15.00
Tier 3 – Supported EMP Applications	$ price on application	$ price on application
Tier 4 – Supported EMP Applications	$ price on application	$ price on application

Monthly Support charges (BYO Supported Devices)

3.11 We will charge you the following monthly support charge for each group of 50 BYO Supported Devices you have. For example, if you have 1 BYO Supported Device we will charge you for 50 BYO Supported Devices, and if you have 51 BYO Supported Devices we will charge you for 100 BYO Supported Devices.

Service component	Number of BYO Supported Devices	Monthly charge per Supported Device (ex GST)	Monthly charge per Supported Device (incl. GST)
Service Desk support (per group of 50 Supported Device)	50	$454.50	$500.00

3.12 Depending on what Enterprise Mobility Managed Service 2 tier you choose, we will also charge you the following monthly support charge for each group of 50 BYO Supported Devices you have. For example, if you have 1 BYO Supported Device we will charge you for 50 BYO Supported Devices, and if you have 51 BYO Supported Devices we will charge you for 100 BYO Supported Devices.

Service component	Number of BYO Supported Devices	Monthly charge (ex GST)	Monthly charge (incl. GST)

Tier 1 – Supported EMP Applications	50	$300.00	$330.00
Tier 2 – Supported EMP Applications	50	$681.82	$750.00

3.13 We determine the number of Supported Devices on the 21st day of the previous month. You acknowledge that your monthly support charge may change each month depending on the number of Supported Devices you have.

Eligibility

3.14 You are only eligible for the Enterprise Mobility Managed Service 2 if you are a Telstra Enterprise and Government customer with an ABN and existing Telstra mobile account. We supply the Enterprise Mobility Managed Service 2 for business purposes and you must use it for predominantly business purposes.

3.15 You can only use the Enterprise Mobility Managed Service 2 if:

(a) you or a person within your organisation has:

(i) an active Enterprise Mobility service provided by us with a properly configured Supported Device that allows you to send and receive e-mail over the internet, browse the internet using the Enterprise Mobility HTML browser or a native application approved and managed by us, and to use our compatible networks for voice calls, text messages and BigPond mobile Enterprise Mobility Managed Services 2 ("**Enterprise Mobility service**") unless otherwise agreed to by us. If we agree to support a device to Users in your fleet that does not meet these criteria ("**Other Users Devices**"), then we will only support Other Users Devices for the following functions:

(A) support from the Service Desk for Incidents and Requests as part of Supported Device, Supported EMP Applications and Supported Hardware support (except to the extent that you have acquired Supported EMP Applications and Functions from us);

(B) Scheduled Maintenance (other than in respect of the EMP); and

(C) Service Management (other than in respect of the EMP);

(ii) a Supported Device that is connected to an EMP that is supplied either by us or by a Supported EMP Vendor; and

(iii) a Supported Device that is approved by us for the purposes of using the

Enterprise Mobility Managed Service 2 ("**User**");

(b) Users acquire and maintain a compatible Enterprise Mobility Managed Service 2 and Supported Device with us;

(c) Users maintain an EMP that is compatible with the Enterprise Mobility Managed Service 2, either with us or with a Supported EMP Vendor;

(d) the Supported Devices are not classified as 'end-of-life' by the Supported Device Vendor and do not have software that is more than 4 releases from the current software recommended by the Supported Device Vendor;

(e) unless we host the EMP, you deploy a connection protocol approved by us for the management and support of the EMP; and

(f) unless we host the EMP, you deploy the EMP monitoring and alerting Enterprise Mobility Managed Services 2 on independent infrastructure to allow us to proactively respond to EMP platform issues.

3.16 Unless otherwise agreed, you are responsible for any hardware, facilities, Supported Devices, accessories or Enterprise Mobility Managed Services 2, and any other telecommunication Enterprise Mobility Managed Services 2 and equipment required to use the Enterprise Mobility Managed Service 2.

Third Party suppliers

3.17 You acknowledge that we may purchase some components of your Enterprise Mobility Managed Service 2 from third party suppliers. If one of our third party suppliers suspends, cancels or terminates a service that we rely on to provide you with your Enterprise Mobility Managed Service 2, we may:

(a) replace or modify your Enterprise Mobility Managed Service 2; or

(b) suspend, cancel or terminate your Enterprise Mobility Managed Service 2 or the affected part.

3.18 We will give you as much notice as is reasonably possible in the circumstances.

3.19 You agree that we may need to provide your contact details and all other necessary information to any third party suppliers we use to provide the Enterprise Mobility Managed Service 2.

Part K – Enterprise Mobility Management

Supported EMP Applications

3.20 You may apply for any one of the following Enterprise Mobility Managed Service 2 tiers as described in the table below:

Tier 1 – Supported EMP Applications*	
1.	MobileIron – Virtual Smartphone Platform (VSP)
2.	MobileIron – Sentry
3.	AirWatch – Mobile Device Management (MDM)
4.	AirWatch – Secure eMail Gateway
5.	Cisco – Cloud Web Security (previously known as Cisco – ScanSafe)
6.	Research in Motion (RIM) - BlackBerry Enterprise Server (BES) 10
7.	Citrix – Mobile Device Management

* If you acquire a Tier 1 - Supported EMP Application you must also have Service Desk support.

Tier 2 – Supported EMP Applications	
1.	AsdeqLabs - AsdeqDocs
2.	NetApp – NetApp Connect

Tier 3 - Supported EMP Applications	
1.	Nil

Tier 4 - Supported EMP Applications	
1.	Nil

3.21 Unless otherwise agreed, your Enterprise Mobility Managed Service 2 only applies to Supported EMP Applications which form part of your chosen Enterprise Mobility Managed Service 2 tier as set out in the tables above. We may change the Supported EMP Applications from time to time on written notice to you.

3.22 You acknowledge that certain features and functionality of a Supported EMP Application may not be available as part of your Enterprise Mobility Managed Service 2.

3.23 Depending on the Supported EMP Application you acquire, you may be required to delegate all administration and access rights for your Supported Devices to the relevant Supported EMP Vendor or other third party supplier approved by us; otherwise we may not be able to provide the Enterprise Mobility Managed Service 2 to you. For example, if you acquire AirWatch – Mobile Device Management as a Tier 1 – Supported EMP

Application, you must delegate all administration and access rights for your Supported Devices to MSC Mobility Pty Ltd or other third party supplier approved by us.

3.24 Unless otherwise agreed, your Enterprise Mobility Managed Service 2 does not include:

(a) Supported Device logistics (excluding activation), procurement, repair or replacement;

(b) Enterprise Mobility Managed Service 2 management; or

(c) Hosting the EMP.

Logon name and password

3.25 We will provide you with a logon name ("Client Number") and password which will provide you with access to the support services and tools which form part of the Enterprise Mobility Managed Service 2.

3.26 You are responsible for ensuring the confidentiality of any Client Number and passwords issued to you as part of the Enterprise Mobility Managed Service 2. We will not be liable for any loss or damage that you or any other person may suffer as a result of your use of the Enterprise Mobility Managed Service 2 or from disclosing your Client Number or password.

Supported Device support

3.27 We will provide Supported Device support, which includes support for Incidents and Requests for the Supported Device Applications and Supported Device hardware functions set out in the "Supported Applications and Functions" section above.

3.28 For the purposes of Supported Device support, the Service Desk will support the following types of Requests, which will also be classified as the following Request categories for the purpose of providing Service Assurance:

Request Type	Request Category
Supported EMP Application: • installation / reinstallation / uninstallation • upgrade / downgrade • update or patch version	IMACD
User changes, being swaps from one Supported Device to another Supported Device	IMACD

Training requests or bookings	RFI – Request for Information
How Do I…? Change a setting, perform a particular function	RFI – Request for Information

3.29 For the purposes of Supported Device support, the Service Desk will support the following types of Incidents, which will also be classified as the following Incident categories for the purpose of providing Service Assurance:

Incident Type	Incident Category
Error or performance issue with accessory (car kit or headset) or accessory connection method such as Bluetooth	Device
Error or performance issue with Supported Device not related to Data Services	Device
Error or performance issue with the audio, volume, vibrations or associated settings on the Supported Device	Device
Error or performance issue with the Keys, Buttons, Trackball, or Touchscreen on the Supported Device	Device
Error or performance issue with the operating system, Supported Device restarts or power offs	Device
Error or performance issue with the phone or call log functions on the Supported Device	Device
Physical damage with the Supported Device – water damage, casing cracked, screen cracked	Device
Error or performance issue with the power, charging or battery functions on the Supported Device	Device
Error or performance issue with profile setup and settings, custom settings and options on the Supported Device	Device
Error or performance issue with the device screen, backlight, screen settings on the Supported Device	Device

Enterprise Mobility Data service support

3.30 We will provide basic Enterprise Mobility Data service support via the Service Desk, which includes support for Incidents and Requests for the Supported EMP Application Functions and services set out in the "Supported EMP Applications and Functions" section above and provided by an EMP to a Supported Device.

3.31 For the purposes of basic Enterprise Mobility Data service support, the Service Desk will support the following types of Requests, which will also be classified as the following Request categories for the purpose of providing Service Assurance:

Request Type	Request Category
• add a User to the EMP – provision Enterprise Mobility Data service on EMP • procurement and delivery of the Supported Device and SIM card (including any compatible car charger, travel kit and holster (**Starter Kit**) • process orders for porting of mobile numbers from one SIM card to another SIM card • process orders for the required mobile voice and data services on a SIM card (including global roaming)	IMACD
Change a User's Account setting on the EMP: • Group • EMP Account settings – PIM Sync, Redirection	IMACD
• delete or remove a User from the EMP • deactivation of the Supported Device and SIM card and disposal of the Supported Device	IMACD
License key changes: • Add CALS / SRP Key(s) • Remove CALS / SRP Key(s)	IMACD
Reset device password on the Supported Device	IMACD
Reactivate Supported Device	IMACD
Disable / Block access / Wipe Supported Device)	Security
Create, Change or Delete an IT / User policy or IT / User policy setting	IMACD (RFC – Request for Change)
How Do I? Change a setting, perform a particular function	RFI – Request for Information

3.32 For the purposes of Enterprise Mobility Data service support, the Service Desk will support the following types of Service Incidents, which will also be classified as the following Service Incident categories for the purpose of providing Service Assurance:

Incident Type	Incident Category
An error or performance issue with address book synchronisation	Data Services
An error or issue performance with a Supported EMP Application	Data Services

An error or performance issue with a Supported EMP Application or service: • Service Name • Domino Service / MAPI Profile	Data Services
An error or performance issue with EMP infrastructure: • Mail Server	Data Services
An error or performance issue with EMP licensing: • CALS Expired • SRP Disabled / Expired	Data Services
An error or performance issue with the Browser Service: • Single Site access • Internet access • Intranet access	Data Services
An error or performance issue with calendar synchronisation	Data Services
An error or performance issue with email synchronisation: • Unable to Receive / Send • Synchronisation • Reconciliation	Data Services
An error or performance issue with instant messaging	Data Services
An error or performance issue with memos / tasks synchronisation	Data Services

3.33 When reporting an Incident or making a Request to the Service Desk you must provide all the information we reasonably require (including completing any service request forms), otherwise we may not be able to resolve the Incident or complete the Request.

Service Desk

3.34 We will operate a service desk for Users to contact ("**Service Desk**") as follows:

Enterprise Mobility Managed Service 2 period	Australian Eastern Standard Time (AEST) or Australian Daylight Savings Time (ADSL)
Business Hours	08:00 – 20:00 Monday to Friday (excluding National Public Holidays)

After Business Hours	20:00 – 08:00 Monday to Saturday; 08:00 Saturday – 08:00 Monday; and National Public Holidays (24 hours)

3.35 Users must contact the Service Desk for all Requests, Incidents and other support in relation to the Enterprise Mobility Managed Service 2 by calling 1800 994 905 or by emailing wireless@team.telstra.com (or such other phone number or email address we tell you from time to time) during the applicable Enterprise Mobility Managed Service 2 Users must contact the Service Desk for all Requests, Incidents and other support in relation to the Enterprise Mobility Managed Service 2 by calling 1800 994 905 or by emailing wireless@team.telstra.com (or such other phone number or email address we tell you from time to time) during the applicable Enterprise Mobility Managed Service 2 period.

3.36 All calls and emails to the Service Desk will be classified as a Request or Incident in accordance with the "Supported Device support" and "Enterprise Mobility Data service support" sections above.

3.37 A User may contact the Service Desk during Out of Business Hours for any Requests or Incidents in relation to:

(a) Supported Device support – but only for Requests in relation to Supported Device passwords and Supported Device disablement (for lost or stolen Supported Devices); and

(b) EMP Incident support – but only for Supported EMP Application monitoring and alert response / resolution.

3.38 The call will be answered by an on-call service and routed to an After Hours Support Engineer who will aim to respond to the User in accordance with the applicable Service Assurance targets. All calls and emails to the Service Desk which are logged After Business Hours will be followed up by the Service Desk the next Business Day during Business Hours.

3.39 If the Service Desk is unable to satisfy the Request or resolve the Incident, it may liaise with any relevant third party suppliers to complete the Request or resolve the Incident on your behalf.

Service Assurance

Availability Targets

3.40 We will aim, but do not guarantee, to meet the following availability targets:

Description	Definition	Target
Service Desk Availability	Service Desk Operational Integrity including systems and process.	99%
Supported EMP Application Availability – Hosted by you (subject to your hardware and network availability)	EMP technology functions including mail routing, 'push' functionality, user management and authentication/authorisation etc.	97%
Supported EMP Application Availability – Turn-Key Hosting by us	EMP technology functions including mail routing, 'push' functionality, user management and authentication/authorisation etc.	Single EMP Server: 97%. EMP Server with warm standby EMP server: 98%. EMP Server pair(s) with Active / Passive LAN Failover: 99%.

Note: EMP service availability is only applicable if we are able to deploy an EMP monitoring and alerting service.

3.41 For the avoidance of doubt, the availability target "Supported EMP Application Availability – Turn-Key Hosting by us" described above is not limited or reduced in any way by the "Request – Response and Restoration Targets" below.

3.42 Availability in a month is calculated as the number of hours for which the Enterprise Mobility Managed Service 2 is available in that month, in accordance with the following formula:

((Scheduled Time - (Downtime - Excusable Downtime)) x 100)/ Scheduled Time

Where:

(a) **"Availability"** means the Enterprise Mobility Managed Service 2 can be accessed or used by one or more Users.

(b) **"Scheduled Time"** in a month means the number of hours specified as hours during which the Enterprise Mobility Managed Service 2 is scheduled to be available.

(c) **"Downtime"** means the number of hours during Scheduled Time in that month during which the Enterprise Mobility Managed Service 2 is not available.

(d) **"Excusable Downtime"** is any scheduled maintenance or planned outage period;

any unavailability of the Enterprise Mobility Managed Service 2 caused by a defect, error or malfunction in any item of hardware, software, configuration or service, and communications not within our control; and any unavailability of the Enterprise Mobility Managed Service 2 caused by an event beyond our reasonable control.

Incident – Response and Restoration Targets

3.43 We will aim, but do not guarantee, to respond and restore an Incident within the following target timeframes:

Severity level	Response Times	Update Frequency	Restoration Times	Target
1 (Critical)	15 min	1 hour	2 hours	90%
2 (Major)	30 min	2 hours	8 hours	90%
3 (Minor)	1 hour	8 hours	2 Business Days	90%

Request – Response and Restoration Targets

3.44 We will aim, but do not guarantee, to respond and restore Requests from a User (or an authorised third party) for information or advice within the following target timeframes:

Request Type	Description	Response	Restoration			Availability	
			Urgent	Standard	Target	Business Hours	After Business Hours
IMACD	User or Device Add/Change/ Delete	1 hour	1 hour*	1 Business Day 2 Business Days**	90%	Yes	No
Security	Kill Pill/ Disable Device/Wipe Device	15 mins***	15mins	30mins	90%	Yes	Yes
How To / RFI	Information Request	1 hour	N/A	3 Business Days	90%	Yes	No

* The Restoration time for Urgent IMACD Requests does not apply where a Device and/or SIM Card and Service needs to be ordered.

** The Restoration time for Standard IMACD Requests to Add Users or Devices will be two Business Days if you acquire the Fleet Management service.

*** The Response time for Security changes will be within 30 minutes After Business Hours.

Quality Targets

3.45 We will aim, but do not guarantee, to meet the following Quality targets in relation to the Service Desk:

Metric	Target
Average Mean Time to Resolution	< 6hrs
GoS - % of calls answered with in 30 secs	80%
Abandoned calls	< 3%
Average Call Handling Time	< 10mins

Note:
Mean Time to Resolution is measured as an average for all Incidents and Requests.
GoS, Abandoned calls and Average Call Handling Time is measured for each inbound phone, not per User.
The above Quality targets are not included in any monthly reporting. If requested, we can provide statistics on these metrics.

Service Assurance terms

3.46 You must provide us with all reasonable assistance in a timeframe which will enable us to

meet the Service Level targets. If you are unable to do so, then the applicable target timeframes will be extended by the amount of time which elapses before you are able to provide the necessary assistance.

3.47 We will not be responsible for a failure to meet any Service Level targets where the failure is caused or contributed to by:

(a) your infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed Service 2;

(b) any unauthorised changes to your technology infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed Service 2; or

(c) an act beyond our reasonable control.

3.48 The following statuses for Incidents and Requests will stop the Service Level clock on a ticket due to an act beyond our reasonable control to continue to resolve the Incident or Request within the applicable Service Level target:

(a) **Waiting for User** – a User has been asked to perform a test or provide feedback on a reported Incident or Request and is not able to immediately provide the feedback or perform the test. The ticket will be placed on this status which stops the Service Level clock. The Service Desk will conduct an outbound follow up via phone or email with the User every 2 days to solicit the feedback and change the ticket status back to **Open** once the feedback has been received.

(b) **With Third Party –** a third party support group is required to perform an action to assist implementation of the Restore or Resolution of the Enterprise Mobility Managed Service 2. The ticket will be placed on this status which stops the Service Level clock. The Service Desk will conduct an outbound follow up via phone or email with the third party every day to solicit the feedback and change the ticket status back to **Open** once the feedback has been received. Where external suppliers or your infrastructure is influencing a delay in Restoration, the Restoration time will increase to the extent of the delay.

(c) **Restored** – the Enterprise Mobility Managed Service 2 has been restored for the User but feedback from the User to confirm the Restore was successful is not immediately available. The ticket will be placed on this status which stops the Service Level clock. The Service Desk will conduct an outbound follow up via phone or email with the User every 2 business days to solicit the feedback and

change the ticket status back to **Open** once the feedback has been received.

(d) **Waiting Change Approval** – a change request has been submitted in accordance with the change and release management process to update a Supported EMP Application and is waiting to be approved, or a ticket has been logged and an Incident is under investigation for root cause.

(e) **Monitoring** – you or your User has agreed to put in place a monitoring period to determine whether an Incident or Request has been resolved.

Scheduled Maintenance

3.49 From time to time we will perform scheduled maintenance in connection with the Enterprise Mobility Managed Service 2, which may involve us interrupting the Enterprise Mobility Managed Service 2 to perform work such as network upgrades, hardware / software modifications or testing. We will provide you with reasonable prior notice.

3.50 You acknowledge that during any scheduled maintenance period you may not be able to retrieve or send email, appointments, data or use other Enterprise Mobility related functions.

3.51 The Service Level targets will not apply in relation to any scheduled maintenance.

Supported Device Fleet Management

3.52 If requested and approved by us, we can provide the following Fleet Management services to track and manage your mobile device fleet:

(a) (a) establish and manage a Supported Device pool for the purpose of replacing faulty Supported Devices and provisioning new Supported Devices;

(b) (b) record and report details of your Supported Device fleet for all your Users; and/or

(c) (c) make recommendations on refreshing your Supported Devices where they are 24 or more months old from the date of purchase and/or based on our assessment on the reliability and serviceability of the Supported Device.

3.53 You must keep the Supported Device pool at a minimum level of 3% of your total Supported Device fleet, provided there are no restrictions on the supply of Supported Devices from Supported Device Vendors.

3.54 We will notify you if we believe the Supported Device pool should be more than 3% of

your total Supported Device fleet. If you do not increase the Supported Device pool following notification from us, the Fleet Management Service Level Targets will not apply.

3.55 We will not be responsible for any Supported Device which is not under our direct control.

3.56 We will charge you the following monthly charge for Supported Device Fleet management depending on the number of Supported Devices you have:

Number of Supported Devices	Monthly Charge (ex GST)	Monthly charge (incl. GST)
1 - 300	$2,500.00	$2,750.00
301 - 700	$5,100.00	$5,610.00
701 - 1400	$7,700.00	$8,470.00
1401 or more	POA	POA

Supported EMP Application - Maintenance and Monitoring

Capacity Management – Monthly User Licence

3.57 We will perform capacity checks for active and inactive Users against your client access licence levels.

3.58 We will provide a monthly report that contains:

(a) (a) Number of active Users;

(b) (b) Number of inactive (not activated / not running) Users; and

(c) (c) Users who have had no contact with the EMP for more than 28 days.

Availability Management – EMP service monitoring

3.59 We will monitor the Supported EMP Application functions and services set out in the table under the heading “Supported EMP Application and Functions” for continuous stoppages of more than 15 minutes, and will generate an alert for each event of this kind. Each alert is generated as an Incident and will be initially logged as a Severity 3 Incident while we conduct further investigations. We will raise the Severity Level upon repeat alerts or if our investigations determine it is a Severity 1 or 2 Incident.

3.60 To ensure consistent performance of the EMP core solution functions such as Email and Organiser Data Synchronisation and Reconciliation, it may be necessary to monitor certain EMP services. If we do not host the EMP, we may require you to provide us with

monitoring capabilities or suitable access to enable us to monitor the Supported EMP Application functions and services.

3.61 To maximise the availability of your Enterprise Mobility Managed Service 2, we recommend you regularly:

(a) perform Database consistency checks to ensure that the Enterprise Mobility Configuration Database (which is the core of the Enterprise Mobility solution and contains your Users' device settings and configuration data) remains stable and avoids corrupted data; and

(b) create an automated ticket to log a Request in relation to each Database consistency check performed in accordance with sub-clause (a) above to confirm whether the check was successful or unsuccessful.

Release Management

3.62 We will use our best endeavours to review each EMP deployment of either an application or a release, upgrade, update or patch (in relation to your EMP service or Supported Device) that has been issued by a Supported Device Vendor and acquired by you from us or the Supported Device Vendor ("**Release**") for applicability and criticality when they are available as a general release from the Supported Device Vendor. If we consider the Release to be relevant to maintaining the availability and security of your EMP service, and provided it does not impact functionality, we will:

(a) test and implement each major EMP Release within 90 days of the Supported Device Vendor making it available as a general release;

(b) test and implement each minor EMP Release within 60 days of the Supported Device Vendor making it available as a general release; and

(c) implement any Supported Device firmware upgrades and/or patching, either prior to Supported Device activation or at the recommendation of the Supported Device Vendor,

in accordance with the change and release management process set out in the "Change and Release Management Process" section below.

Change and Release Management Process

3.63 You must notify us of any planned changes to the platform and its services, including the operating system, back-ups, anti-virus and security as follows:

(a) for regular changes, you must provide us with at least 14 days prior notice; and

(b) for emergency changes, you must provide us with at least 8 Business Hours' notice.

3.64 Each change or Release requested by either you or us (including any changes to the EMP configuration) must be agreed before it is implemented. We will not agree a change until the following actions have been completed to our reasonable satisfaction:

(a) change definition completed;

(b) change windows identified, including resource availability (physical and technical);

(c) change tasks defined;

(d) roll-back tasks defined;

(e) test plan defined;

(f) test plan actioned, including roll-back plan (subject to constraints notified by us);

(g) change window confirmed (release date);

(h) Service Desk is notified of the release date;

(i) you have informed us that internal approval has been provided by each of your internal representatives concerned with the change; and

(j) each of our representatives and specialists has approved the change.

3.65 You must not make any changes to the infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed Service 2 without complying with this "Change and Release Management Process" section. You indemnify us against all losses, damages, expenses and costs suffered or incurred by us arising out of, or in connection with, your failure to comply with this "Change and Release Management Process" section.

Service Management

3.66 If requested and approved by us, for an additional charge we can provide the following Service Management services to you, which will be set out in your separate agreement

with us:

(a) **Standard Service Management** – allocation of a Service Delivery Coordinator for service escalations, and participation in a monthly operational meeting; or

(b) **Enterprise Service Management** – allocation of a Service Delivery Manager for service escalations and service management, and participation in a monthly operational meeting and monthly service review meeting.

Law of Large Numbers

3.67 Because percentages become less accurate for displaying results the smaller the number becomes, if the total number of tickets logged for a particular category of Incident or Request is less than 40, the below table will be used to measure and display Service Level results for reporting in accordance with the section above under the heading Change and Release Management Process.

Total Number of Tickets Logged	**Allowable Ticket Failures**	Ticket Failures / Enterprise Mobility Managed Service 2 Service Level result		
		Failure to meet Enterprise Mobility Managed Service 2 Service Level Targets	Enterprise Mobility Managed Service 2 Service Level Targets achieved	Enterprise Mobility Managed Service 2 Service Level Targets exceeded
1 to 10	1	≥ 2	1	0
11 to 20	2	≥ 3	2	≤ 1
21 to 30	3	≥ 4	3	≤ 2
31 to 40	4	≥ 5	4	≤ 3

Note: Service Level results are measured and displayed by the number of ticket failures compared to the total with an allowable number of failures per range of 10 tickets.

Fleet Management Service Level Targets

3.68 We will aim, but do not guarantee, to meet the following service level targets for the following fleet management services outlined below:

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Mobile device delivery for up to 100 new service connections. (For orders of mobile devices and accessories for more than 100 new service connections, this service level target will not apply. We will discuss and agree a delivery time with you).	This service level target **only** applies to: • email orders from Users; and • email orders from Users with Other Devices which are directed to and received by Service Desk. **Note:** An order must be submitted for each individual device.	**For delivery of 90% of new mobile devices** Provided the Enterprise Mobility Managed Service Desk receives your completed **email or electronic order** on a business day before 12.00pm (AEST): • Delivery to **Metropolitan** areas – next business day following receipt of your order; • Delivery to **Regional** areas – within 2 business days following receipt of your order; and • Delivery to **Remote** areas - within 5 business days following receipt of your order. **Note:** There are no deliveries on weekends or public holidays. Next day delivery may not be possible in the circumstances where the mobile device model requested by you is out of stock or is not available from the manufacturer; the mobile device model requested by you has been discontinued; we are unable to deliver the mobile device to you because your delivery address is incorrect or incomplete; we are unable to gain access to your site to deliver the mobile device to you, or for any reason beyond our reasonable control.

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Faulty mobile device repairs	This service level target **only** applies to: • email orders from Users; and • email orders from users with Other Devices which are directed to and received by the Service Desk. **Note:** An order must be submitted for each individual device.	**For 90% of faulty mobile devices:** Repair and delivery • Spare Pool location in **Metropolitan** areas – within 11 business days from receipt of your mobile device by the Telstra Repair Centre; and • in all other areas – within 20 business days from receipt of your mobile device by the Telstra Repair Centre. **Note:** There are no deliveries on weekends or public holidays. This service level target does not apply if: • replacement parts are not available for your mobile device from the mobile device manufacturer; or • the Enterprise Mobility Managed Service Desk determines that your mobile device needs to be returned to the mobile device manufacturer for repair.

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Replacement of lost or stolen mobile devices	This service level target **only** applies to: • email orders from Users; and • electronic orders from Users with Other Users Devices which are directed to and received by the Service Desk. **Note:** An order must be submitted for each individual device.	**For delivery of 90% of replacement mobile devices** Provided that the Enterprise Mobility Managed Service Desk receives your completed **email or electronic order** on a business day before 12.00pm (AEST): • Delivery to **Metropolitan** and **Regional** areas – next business day following receipt of your order; and • Delivery to **Remote** areas - within 5 business days following receipt of your order. **Note**: There are no deliveries on weekends or public holidays. Delivery within the above timeframes may not be possible in the circumstances where the mobile device model requested by you is out of stock or is not available from the manufacturer; the mobile device model requested by you has been discontinued; we are unable to deliver the mobile device to you because your delivery address is incorrect or incomplete; we are unable to gain access to your site to deliver the mobile device to you, or for any reason beyond our reasonable control.

3.69 The above service level targets will not apply:

(a) if you order mobile devices, services or activations through any delivery channel other than the Enterprise Mobility Managed Service Desk; or

(b) to any orders received in relation to Other Users Devices (as described in clause above under the heading "Eligibility").

Additional Services

3.70 For an additional fee, you may also purchase additional services in the form of:

(a) 24/7 Service Support;

(b) Managed App Services (MAS); and

(c) Managed App Reputation Scanning (MARS),

together the (Additional Services).

3.71 The Additional Services are only available to Customers with an existing EMMS service (which may include T-MDM or supported MDM).

24/7 Service Support

3.72 We will operate a 24 hour, seven day a week service desk (24/7 Service Support) for your company's staff to contact which includes the full capabilities of the Service Desk but on a 24/7 operational cycle and is available for all Enterprise Mobility Managed service packages.

3.73 Users must contact 24/7 Service Support for all Requests, Incidents and other support in relation to the relevant Enterprise Mobility Managed service by calling 1800 994 905 or emailing support@mscmobility.com.au (or such other phone number or email address as notified by us from time to time) during the applicable Enterprise Mobility Managed service period.

3.74 All calls and emails to 24/7 Service Support will be classified as a Request or Incident in accordance with relevant clauses beginning at clause 3.27.

3.75 If 24/7 Service Support is unable to satisfy the Request or resolve the Incident, it may liaise with any relevant third party suppliers to complete the Request or resolve the Incident on your behalf.

3.76 We aim, but do not guarantee, to make 24/7 Service Support available in accordance with the Availability Targets set out in the relevant clauses beginning at clause 3.40.

Service Matrix

3.77 The 24/7 Service Support includes the following functionality:

Service Desk – General Service Access	
Email and Phone Support	Tickets can be logged with Telstra via phone or email as per the Service Desk phone number and email address respectively. It is recommended that End Users use phone support for After Business Hours (urgent / business critical incidents).

Part K – Enterprise Mobility Management

End User Service Desk – Level 1 First Point of Contact	A Level 1 Service Desk service with direct End User support. All incidents and requests are directed to Telstra who will manage resolution and escalation.
IT Service Desk Support – Level 2 and Level 3 IT Escalations	A Level 2 and 3 Service Desk for escalations from a Telstra Customer's IT service desk. All MDM administration is performed by our 3rd party.
MDM Administrator Support	A Level 3 Service Desk for Business Critical Severity 1 incidents and MDM console access incidents ONLY.
Product Vendor Escalations and Management	Product Vendor related incidents are escalated to the Product Vendor and managed by Telstra's 3rd party where required.

Service Items	Description	Service Desk		24/7 Support Services
		Business Hours	After Hours	24/7
		08:00 – 20:00 MF	20:00 – 08:00 SM	0:00 – 23:00 SM
Incident and Request Management				
Mobile Device Support – Incidents and Request	Support for Device Related Services and Functions	✓		✓
MDM Platform Support — MDM Configuration Requests	Function or application related to Configuration on the MDM Server (This could be a user or platform configuration on the MDM Server).	✓		
Carrier Support Escalations — Incidents and Requests	Managed escalations to your Network Carrier for SIM Card Service Requests and Incidents.	✓		✓
MDM Vendor Escalations – Incidents and Requests	Managed escalation to Product Vendors for MDM platform related queries and / or issues	✓		✓
MDM Platform Support – Incidents ONLY	Support for Business Critical Severity 1 incidents ONLY	✓	✓	✓
24/7 Mobile Device Support - Requests for Password Resets and Lost and Stolen - Data Wipe Only	Support for Password Resets and Lost or Stolen Devices ONLY	✓	✓	✓
24/7 Mobile Device Support – Incident and Service Requests for Roaming Users	Support for Roaming Users for Incidents and Requests. User MUST be travelling temporarily overseas	✓	✓	✓
Release and Change Management				

Part K – Enterprise Mobility Management

MDM Policy Breach Management	Monitoring of MDM Policy breaches on devices and management of resultant actions of policy breach	✓		✓
Release and Change Management — Patch and Maintenance Releases	Maintenance Releases and Patching are performed for the selected MDM Platform	✓		
Availability Management — Platform Service Monitoring	Platform Monitoring for Service Uptime and Unplanned Outages	✓	✓	✓
High Priority Incident Management	Support for incidents that require a higher tier support group due to the incident severity pertaining to urgency and impact	✓	✓	✓
Service Management				
Single Point of Contact Service Management	A Service Delivery Manager is assigned to your account providing a single point of contact for escalations, ad hoc business Q&A and service management tasks	✓	✓	
Monthly Service and Ticket Reporting	A Monthly Report detailing performance against Service SLA's and recommendations on improving the service	✓		
Monthly Service Review Meeting	A Monthly meeting to review the monthly report and discuss items in the service	✓		
High Priority Incident Management contact	Single point of contact coordination and stakeholder communications during High Priority Incidents (including Afterhours duty SDM)	✓	✓	✓
Continual Service Improvement	Management of process enhancements and Service Improvements Programs	✓		
Fleet Management (all service items below are optional)				
Device Procurement & Logistics	Management of Device Ordering, Fulfilment and any Logistics in relation to Device Ordering	✓		
Device Staging and Deployment	Management of the device staging and MDM enrolment processes prior to delivering to the End User	✓		

Device Repair and Replacement Management	Management of device hardware faults, repair processes, and a device spare pool for device replacements	✓		
Fleet Location Management and Tracking	Management of device to user assignments and locations of devices.	✓		
Asset Reporting	An additional section in the monthly report detailing asset (device) movements for the month	✓		

24/7 Service Support – Pricing

3.78 24/7 Support Service charges:

24/7 Service Support Components	Low	Medium	High
Per Month Access (GST Exclusive)	$2,500.00	$5,000.00	POA
Per Month Access (GST Inclusive)	$2,750.00	$5,500.00	POA
Per Ticket (GST Exclusive)	$150.00	$125.00	POA
Per Ticket (GST Inclusive)	$165.00	$137.50	POA
Fair Use Policy (FUP)*	20 tickets	50 tickets	POA

Note:

- *Fair Use Policy (FUP) – has been designed to meet the organisational requirements of Customers. This tiered pricing includes the FUP that indicates the ticket per month allowance.
- 24/7 Service Support ticket reports will be generated monthly and provided through Service Delivery Management channels.
- End User app support service consumption is reviewed monthly and adjustments are negotiated quarterly.
- This product has been developed for existing EMMS Customers but is also available to new EMMS Customers.

Managed App Services (MAS)

3.79 MAS is a suite of services incorporating app procurement, deployment, configuration, security, reporting, compliance and support. It also provides an optional capability to have a managed service wrapped around Bespoke Enterprise App Management for Telstra preferred app developers that can assist in the complex change management of bespoke app deployment and support.

Part K – Enterprise Mobility Management

3.80 MAS includes:

(a) Service Design, Build & Implementation (Mandatory Customer requirement)

(b) Public Business and Productivity App Matching

(c) Corporate App Store Branding & Management

(d) Corporate App Procurement Service

(e) MAS - Reporting

(f) MAS - Ongoing Maintenance and Upgrades

(g) Bespoke Enterprise App Management - Optional

Service Design, Build & Implementation (Mandatory Customer requirement)

3.81 Service Design and build process consists of an introductory meeting between you and Telstra representatives) to define and design the MAS as per your business requirements. We will manage the end to end design of the service, implement and activate the required components. The process includes the following:

(a) Project Scoping

(b) Agreed Service Design & Statement of Work

(c) Build, test, pilot & sign off

(d) Service Transition & on boarding

(e) EMMS Platform Configuration

(f) Public App Management (Optional)

Public Business and Productivity App Matching

3.82 We will consult with you to define a policy around how public apps are managed on your device fleet to understand current app usage by Users, define a list of same or equivalent apps that allow business continuity to be pushed out to Users and which can be automatically or manually updated over Wi-Fi or cellular networks.

Part K – Enterprise Mobility Management

Corporate App Store Branding & Management

3.83 Supplier will define and build a corporate branded App store as a single go to reference for End Users to retrieve recommended business and productivity apps for the End User. The corporate app store will be pushed down over the air and may incorporate the Customer's corporate logo and or colours if required (platform dependent).

Corporate App Procurement Service

3.84 We will provide an app procurement service for you to enable you to purchase and deploy paid public apps which can be licensed, billed and registered to your business. We may also assist in the integration of the app store licensing to EMMS supported platforms and push these apps over the air or remove them when required from your Users' devices (iOS Devices only).

MAS - Reporting

3.85 We will report to you monthly on applicable service level utilization and implementation which will include the following:

(a) Project Management Implementation;

(b) Apps deployed on EMMS platforms;

(c) App version information;

(d) Corporate App Store Apps;

(e) Bespoke Enterprise Managed Apps; and

(f) Paid Public App Licensing.

MAS - Ongoing Maintenance and Upgrades

3.86 We will provide ongoing maintenance of the Managed App Service including Corporate App Store Management, Procurement and Management of Apps & Public App Management. From time to time we may also be required to undertake any underlying platform upgrades to maintain the Managed App Service.

3.87 You acknowledge that during any scheduled maintenance period you may not be able to retrieve or use apps or other Enterprise Mobility related functions.

3.88 Any Service Level targets will not apply in relation to any scheduled maintenance.

Bespoke Enterprise App Management - Optional

3.89 The Bespoke Enterprise App Management provides you with support to build and deploy enterprise apps for End Users. We provide the managed services to work with app developers to ensure that apps are deployed correctly, maintained and meet your corporate compliance standards and are effectively supported.

3.90 We will work with our preferred app developers to provide you the following:

(a) service design - build a level of service to meet your business requirements based on the supported app;

(b) secure app retrieval from the developer – we will work with the supported developer to ensure that app code is transferred in a secure method to the EMMS platform;

(c) app deployment through EMMS supported platforms - creation of group and device deployment polices (including basic testing) to User devices over the air and app updates when required within fair use policy.

(d) change & release management - manage timing of releases with the supported app developers to manage app deployment, changes and updated to software;

(e) user credentials field injection for supported apps - where supported, We can populate app settings on mass with user credentials which can significantly increase User experience;

(f) User support for Bespoke Enterprise Managed Apps - Users may call the Service Desk for bespoke Enterprise App Support for which we will endeavour to provide assistance at first call;

(g) basic app troubleshooting and escalation – We will provide basic app troubleshooting services with defined apps for Users; and

(h) ticket management for supported Bespoke Enterprise Managed Apps – where required, we will escalate support to the app developer and manage the service ticket until close within standard SLA’s as set out in clauses 3.40 onward.

Part K – Enterprise Mobility Management

Managed App Services charges:

3.91 The Managed App Service charges are as follows:

Managed App Service Components	Charges (GST Exclusive)		Charges (GST Inclusive)			
Public App Management						
Service Design, setup and Implementation. Once off setup fee.	$5000.00		5,500.00			
Public App Management Service Fee - per month	$2000.00		$2,200.00			
Bespoke Enterprise App Management						
	1 - 5 Apps (GST Exclusive)	1 - 5 Apps (GST Inclusive)	6 - 10 Apps (GST Exclusive)	6 - 10 Apps (GST Inclusive)	10 + Apps, (GST Exclusive)	10 + Apps (GST Inclusive)
Bespoke Enterprise App Deployment - per app	$4000	$4,400	$4000	$4,400	POA	POA
App maintenance – per app per month (incl. 2 changes per month)	$1500	$1650	$1250	$1,375	POA	POA
Additional changes thereafter per request	$500	$550	$500	$550	POA	POA
App Support Service Consumption rates	2.00% ticket rate	2.00% ticket rate	2.63% ticket rate	2.63% ticket rate	2.8% ticket rate	2.8% ticket rate

User Service Desk Support - per app, per month.*	$1.55	$1.71	$1.85	$2.04	$2.15	$2.37

Note:

- User app support measured as tickets raised per app per month as a % of each app in deployed population.
- All End User app support services start at reference rate of 2.8%.
- End user app support service consumption is reviewed monthly and adjustments are negotiated quarterly.
- End user app support service fees may be higher or lower than the listed fees if very high or very low consumption rates occur in the support trend.

Managed App Reputation Scanning (MARS) service

3.92 The MARS Service is an optional feature of the Managed App Service which is only available to EMMS Customers who have T-MDM or another supported MDM.

3.93 The MARS Service includes:

(a) Service Design, Setup & Implementation

(b) Integration & Management; and

(c) MARS Reporting and Ongoing Management

MARS Service Design, Setup & Implementation

3.94 Service Design and Setup consists of an introductory meeting with you to define and design the Managed App Reputation Scanning solution tailored to your requirements. We will manage the end to end design of the service, implementation and activate the required components which include the following:

(a) Project Scoping;

(b) Security policy design;

(c) Escalation process design and remediation rules;

(d) Agreed Service Design & Statement of Work;

(e) Build, test & sign off; and

(f) Service Transition & on boarding.

3.95 We will provide identification of apps which we believe may show signs of risky behaviour and are therefore a security or stability threat to your device fleet. We will automatically remediate them based on your business security requirements and build appropriate policy to follow in the future as well as provide regular app security updates reports.

3.96 As part of our Security Policy Design, we will develop remediation actions, policy definition, whitelisting and blacklisting of apps to maintain security standards taking into account a balance between risk and your users' experience.

MARS Integration & Management

3.97 EMMS & App Reputation Scanning Integration: We will integrate the cloud hosted App Reputation Scanning engine with the existing EMMS platform (including where you who have selected T-MDM or other supported platform as your MDM platform) which requires the installation and configuration of the scanning engine with the MDM platform for reporting.

3.98 The App Reputation Scanning Engine hosting is included in the Managed App Service.

MARS Reporting and Ongoing Management

3.99 Reporting: We will provide monthly reporting in discussion with you around app risk analysis which will be delivered through service management by performing the following:

(a) Devices scanned & under management;

(b) Unique apps in the device environment;

(c) App risk violations report;

(d) Top 10 riskiest apps;

(e) Policy violation intelligence;

(f) Risk reduction intelligence;

(g) Policy management; and

(h) Tailored compliance remediation review.

3.100 Ongoing Management and Maintenance: As a part of our ongoing maintenance of the Managed App Reputation Scanning Service, We will maintain the MARS service for you which includes app scanning, updates, integration and policy management and we will ensure that any underlying platform upgrades are performed to maintain the Managed App Reputation Scanning Service.

3.101 Managed App Reputation Scanning – Pricing: The following charges apply for the Managed App Reputation Scanning service:

Managed App Reputation Scanning Service			
Volume	**5000**	**5001-10,000**	**10,000+**
Service Design, setup and Implementation. Once off setup fee. **(GST Exclusive)**	$10,000	$10,000	POA
Service Design, setup and Implementation. Once off setup fee. **(GST Inclusive)**	$11,000	$11,000	POA
Monthly Service Fee per Supported Device **(GST Exclusive)**	$2.50	$2.00	POA
Monthly Service Fee per Supported Device **(GST Inclusive)**	$2.75	$2.20	POA

MARS Minimum Term

3.102 If you take up MARS as part of your Enterprise Mobility Managed Service 2 on or after 20 November 2016, you must do so for a minimum term of 12 months (MARS Minimum Term). If your Enterprise Mobility Managed Service 2 or MARS is cancelled or terminated during the MARS Minimum Term other than for our breach your agreement with us, early termination charges (MARS ETCs) will apply for MARS.

3.103 The ETC will be calculated as follows:

A x B x C x 0.75= ETC

where:

A is the applicable Monthly Service Fee per Supported Device for your MARS;

B is your number of Supported Devices; and

C is the number of months remaining (or part thereof) of the MARS Minimum Term.

Other professional services

3.104 If requested and approved by us, we can provide the following professional services which will be set out in your separate agreement with us.

Description	Charge (ex GST)	Charge (incl. GST)
Mobility Consulting – Advisory	$10,500	$11,550
Mobility Consulting – Security / Device Management	$6,000	$6,600
EMMS – Cloud and T-MDM Integration	$10,500	$11,550
EMMS – Integrated Cloud	$17,000	$18,700
EMMS – On premise (uplift)	$6,500	$7,150
Device Deployment options		
Standard Device Deployment	$7,000	$7,700
Advance Device Deployment (per service)	$80	$88
T- MDM Bundles		
T-MDM Quick Start	$5,500	$6,050
T- MDM Advanced Configuration	$10,500	$11,550

Your obligations

3.105 You must nominate a person to be your single point of contact with us for all matters in relation to the Enterprise Mobility Managed Service 2.

3.106 Unless otherwise specified as part of your Enterprise Mobility Managed Service 2 package, you and your Users are responsible for the purchase of any Enterprise Mobility service, Supported Devices and accessories, and any other ancillary products and services.

3.107 Unless we host the EMP, you must not prevent us from connecting to the EMP server located on your premises for the purpose of us providing the Enterprise Mobility Managed Service 2, unless the method of connection:

(a) (a) breaches your documented IT security policy for remote connections;

(b) (b) poses a significant and tangible threat to your business operations; or

(c) (c) your Enterprise Mobility Managed Service 2 has been terminated.

3.108 You acknowledge that mechanisms and procedures that you may use for the purpose of

establishing secure external third party connections may hinder or prevent us from providing the Enterprise Mobility Managed Service 2. If so, the parties will work together in good faith to implement a suitable external third party connection scheme that will enable us to provide the Enterprise Mobility Managed Service 2.

3.109 You:

(a) must not resell or resupply the Enterprise Mobility Managed Service 2;

(b) unless we host the EMP, are responsible for the platform and its services including the operating system, back-ups, anti-virus and security. Backups should include the SQL database, Supported EMP Applications and the operating system;

(c) must not make any unauthorised changes to any infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed Service 2 without complying with the change and release management process set out in the section under the heading Change and Release Management Process above;

(d) must promptly notify us of any changes to your technology environment which may impact the Enterprise Mobility Managed Service 2, including any changes to your email infrastructure and network (such as firewalls and gateways);

(e) must provide us (or our suppliers or representatives) with all reasonable assistance and access to your information, premises, systems and equipment (including Supported Devices) as requested by us from time to time in connection with us providing the Enterprise Mobility Managed Service 2; and

(f) must comply with all our reasonable instructions and procedures in relation to the Enterprise Mobility Managed Service 2 as advised or notified to you.

3.110 You must ensure that you have sufficient security infrastructure in place to prevent email viruses, denial of service attacks and other malicious digital attacks. We will not be liable for any loss or damage that you or any other person may suffer as a result of:

(a) your Supported Devices; or

(b) unless we host the EMP, EMP infrastructure,

(c) becoming infected with a virus, malware or other form of malicious software.

3.111 If we need to attend your premises in relation to the Enterprise Mobility Managed Service 2, you must ensure that our personnel (or our representatives) are provided with a safe and

appropriate working environment when working on your premises.

3.112 You warrant that your use of the Enterprise Mobility Managed Service 2 will not:

(a) breach any law, regulation, industry code or standard; or

(b) infringe the rights of any third party.

3.113 You indemnify us against all losses, damages, expenses and costs suffered or incurred by us arising out of, or in connection with, your failure to comply with this "Your Obligations" section.

Using your Device overseas

3.114 You acknowledge that you could breach the laws of another country (in particular the United States or Canada) if you use, send or take a Supported Device outside of Australia. This is partly due to laws regulating the importation, exportation and use of encryption software embedded within a Supported Device.

3.115 You may only use a Supported Device in, or send or take it to or from, other countries approved by us for your network. We will provide a list of approved countries for Supported Devices on the telstra.com website, which we may update from time to time.

Password protection

3.116 Each Supported Device has a password protection function. You must make sure that this function is always activated on your Supported Device, regardless of who is using it.

Responsibility for use of the Enterprise Mobility Managed Service 2

3.117 You are solely responsible for your use of the Enterprise Mobility Managed Service 2 and the content and security of any data or information which is sent or received using your Supported Device and the Enterprise Mobility Managed Service 2.

Acceptable Use Policy

3.118 You must use your Supported Device, our services and our networks in accordance with our Acceptable Use Policy (as we vary it from time to time) which is available at www.telstra.com. We may suspend or terminate your access to our networks if we reasonably believe that you are in breach of our Acceptable Use Policy. We will tell you before this happens.

Special Meanings

3.119 The following words have the following special meanings:

(a) **Incident** means an event which is not part of the standard operation of a service and which causes or may cause disruption to a reduction in the quality of services and User productivity, as described in the sections above entitled Supported Device support and Enterprise Mobility Data service support.

(b) **Metropolitan Area** or **Metropolitan** means the metropolitan areas in Sydney, Canberra, Melbourne, Brisbane, Perth, Hobart and Adelaide.

(c) **Request** means a request from a User (or an authorised third party) for information or advice, as described in the sections above entitled Supported Device support and Enterprise Mobility Data service support.

(d) **Response** occurs when action is taken to assign an Incident or Request ticket and an email is sent to the requestor to inform them the Incident or Request has been received and assigned to an individual person for resolution.

(e) **Restoration** occurs when action is taken to implement and confirm that the User has the required level of Enterprise Mobility Managed Service 2 working to perform their job role or function (E.g. restore an email sending incident so the User can send email from their Supported Device). Restoration may be implemented by performing a workaround or temporary resolution which will be followed up at a later date and have a permanent resolution implemented or may be implemented using a permanent resolution.

(f) **Severity 1 (Critical)** means failure of the system with a major business impact affecting more than one User, business critical system or process with no workaround.

(g) **Severity 2 (Major)** means one or more Users are affected by the failure of a business critical system or Supported EMP Application which may have a workaround that cannot be sustained over a reasonable period of time (more than 1 day).

(h) **Severity 3 (Minor)** means one User is affected and not business critical which may have a workaround that can be sustained over a reasonable period of time (more than 1 day).

(i) **Standard Request** means there is no immediate impact and the request is not

business critical.

(j) Supported Device means:

(k) an eligible BlackBerry device that is manufactured by Research in Motion Limited (**RIM**) and approved by us, including the BlackBerry devices running BlackBerry operating system versions from 7.x minus 4 versions and BlackBerry devices running operating system versions 10.x and above;

(l) an eligible smartphone device that is manufactured by a Supported Device Vendor and which is approved by us and notified to you in writing from time to time, including the Apple iPhone MC131X or later model, Apple devices running iOS 3.1 or later version, devices using the Windows Phone 7 and Windows Phone 8 operating system, and devices using the Android operating system; and

(m) any other eligible mobile and smartphone devices that are approved by us.

(n) We may change the Supported Device from time to time on written notice to you.

(o) **Supported EMP Application** means an eligible software application supplied by a Supported EMP Vendor which is approved by us and compatible with the Enterprise Mobility Managed Service 2, and which form part of the Enterprise Mobility Managed Service 2 tiers. We may change the Supported EMP Applications from time to time on written notice to you.

(p) **Supported EMP Vendor** means an eligible vendor that supplies EMP services that are approved by us and compatible with the Enterprise Mobility Managed Service 2, and which form part of the Enterprise Mobility Managed Service 2 tiers. We may change the Supported EMP Vendors from time to time on written notice to you.

(q) **Supported Device Vendor** means a vendor that manufactures Supported Devices, including Apple Pty Limited and Apple Inc. We may change the Supported Device Vendors from time to time on written notice to you.

(r) **Urgent Request** means there is an immediate impact and / or the request is business critical.

4 Enterprise Mobility Managed Service

Enterprise Mobility Managed Service is not available to customers who sign a new Enterprise Mobility Managed Service agreement on and from 1 February 2014,

unless otherwise agreed).

What is the Enterprise Mobility Managed service?

4.1 Our Enterprise Mobility Managed service provides monitoring, management, maintenance and user support services by way of a managed application layer for eligible customers in relation to Enterprise Mobility services and eligible Supported Handsets. We also provide a service desk for the purposes of supporting the Enterprise Mobility Platform. You may also purchase Additional Services as set out in these terms.

4.2 You may apply for any one of the following Enterprise Mobility Managed service packages (**Enterprise Mobility Managed service**):

(a) Entry Level Package

(b) Base package;

(c) Premium package; or

(d) Premium Plus package.

4.3 Unless otherwise specified as part of your Enterprise Mobility Managed service package, the Enterprise Mobility Managed service does not include:

(a) Supported Handset logistics (excluding activation), procurement, repair or replacement;

(b) Enterprise Mobility Managed service continuity management; or

(c) Hosting the Enterprise Mobility Platform.

What is the Enterprise Mobility Platform?

4.4 The Enterprise Mobility Platform is the component of the Enterprise Mobility Managed service solution that either provides corporate wireless data synchronisation and device management services to Supported Handsets, or manages the corporate wireless data synchronisation and device management services to Supported Handsets. The Enterprise Mobility Platform is made up of server infrastructure, an operating system and an enterprise mobility platform application.

4.5 If you would like to apply for an Enterprise Mobility Managed service to support Supported Handsets (other than BlackBerry handsets), you must connect the handsets to an Enterprise Mobility Platform. The Enterprise Mobility Platform can either be hosted by

us or by a Supported EMP Vendor approved by us (to ensure the Supported EMP Vendor's Enterprise Mobility Platform is compatible with your Enterprise Mobility Managed service).

(a) If the Enterprise Mobility Platform is hosted by us or Supported EMP Vendor, certain terms below regarding the Enterprise Mobility Managed service will not apply to you (as specified below).

(b) If you choose for the Enterprise Mobility Platform that is not hosted by us or by a Supported EMP Vendor in order to allow compatibility with our systems and the Enterprise Mobility Managed Service that we provide, you may be required to agree to an End User Licence Agreement (**EULA**) in relation to the Enterprise Mobility Managed service with Mobile Iron, Inc. (as amended from time time) or another third party approved by us. You may obtain a copy of the EULA from us upon your request.

Minimum Term

4.6 You must take the Enterprise Mobility Managed service for a minimum term of 24 months.

If your Enterprise Mobility Managed service is cancelled or terminated for any reason (other than for our material breach) during the minimum term, we may charge you an early termination charge calculated as follows:

A x B x 25%

Where:

"A" means the average service charges paid or payable each month by you for the Enterprise Mobility Managed service up to the date of cancellation or termination.

"B" means the number of months (or part of a month) remaining in the minimum term.

You acknowledge that this amount is a genuine pre-estimate of the loss that we are likely to suffer.

Service charges

4.7 You must pay us the Enterprise Mobility Managed service charges specified below. For the avoidance of doubt, these service charges do not include any charges for any underlying telecommunications services used in connection with the Enterprise Mobility

Managed service.

Monthly Support charges (Entry Level package)

4.8 The Minimum monthly service fee for Entry Level package is

Service description	Monthly Charge (ex GST)	Monthly Charge (incl. GST)
Minimum monthly service fee	$600	$660

4.9 The Entry Level package per user charge will be specified in your Application Form or other agreement with us.

Monthly Support charges – (Base, Premium and Premium Plus Packages - for connections before 27 July 2011)

4.10 If you connected to the Base, Premium or Premium Plus package before 27 July 2011, we will charge you the following Monthly Support Charges for using the Enterprise Mobility Managed service charges.

Service description	Monthly Charge (ex GST)	Monthly Charge (incl. GST)
Base Package		
Minimum monthly service fee	$250	$275
Base package	$11 per User	$12.10 per User
Premium Package		
Minimum monthly service fee	$250	$275
Premium package	$16 per User	$17.60 per User
Premium Plus Package		
Minimum monthly service fee	$1,500	$1,650
Premium Plus package	$26.00 per User	$28.60 per User

Monthly Support charges – (Base, Premium and Premium Plus Packages - for connections on or after 27 July 2011)

4.11 If you connected to the Base, Premium or Premium Plus package on or after 27 July 2011, we will charge you the following Monthly Support Charges for using the Enterprise Mobility Managed service charges:

Part K – Enterprise Mobility Management

Service description	Monthly Charge (ex GST)	Monthly Charge (incl. GST)
Base Package		
Minimum monthly service fee	$250	$275
Base package	$13.64 per User	$15.00 per User
Premium Package		
Minimum monthly service fee	$454.50	$500.00
Premium package	$18.18 per User	$20.00 per User
Premium Plus Package		
Minimum monthly service fee	$590.91	$650
Premium package	$23.64 per User	$26.00 per User

Eligibility

4.12 You are only eligible for the Enterprise Mobility Managed Service if you are a business or corporate customer.

4.13 You can only use the Enterprise Mobility Managed service if:

(a) you or a person within your organisation has:

(i) an active Enterprise Mobility service provided by us with a properly configured Supported Handset that allows you to send and receive e-mail over the internet, browse the internet using the Enterprise Mobility HTML browser and to use our compatible networks for voice calls, text messages and BigPond mobile Enterprise Mobility Managed services (**Enterprise Mobility service**) unless otherwise agreed to by us. If we agree to support a handset to users in your fleet that does not meet this criteria (**Other Users Devices**) then we will only support Other Users Devices for the following functions:

(A) support from the Service Desk for incidents and requests as part of Supported Handset Applications and Supported Hardware support (except to the extent that you have acquired Supported EMP Applications and Functions from us);

(B) Scheduled Maintenance (other than in respect of the EMP); and

(C) Service Management (other than in respect of the EMP)

(ii) a Supported Handset that is connected to an Enterprise Mobility Platform

that is supplied either by us or by a Supported EMP Vendor; and

(iii) a Supported Handset that is approved by us for the purposes of using the Enterprise Mobility Managed service (**User**);

(b) Users acquire and maintain a compatible Enterprise Mobility Enterprise Mobility Managed service and Supported Handset with us;

(c) Users maintain an Enterprise Mobility Platform that is compatible with the Enterprise Mobility Managed service, either with us or with a Supported EMP Vendor;

(d) the Supported Handsets are not classified as 'end-of-line' by the Supported Vendor and do not have software that is more than 4 releases from the current software recommended by the Supported Vendor;

(e) unless we host the Enterprise Mobile Platform, you deploy a connection protocol approved by us for the management and support of the Enterprise Mobility Platform; and

(f) unless we host the Enterprise Mobility Platform, you deploy the EMP monitoring and alerting Enterprise Mobility Managed services on independent infrastructure to allow us to proactively respond to EMP platform issues.

4.14 Unless otherwise specified as part of your Enterprise Mobility Managed service package, you are responsible for any hardware, facilities, Supported Handsets, accessories or Enterprise Mobility Managed services, and any other telecommunication Enterprise Mobility Managed services and equipment required to use the Enterprise Mobility Managed service.

Supported Applications, Functions and Enterprise Mobility Managed Services

4.15 The Enterprise Mobility Managed service only applies in relation to the applications, functions and Enterprise Mobility Managed services set out below or otherwise approved by us in writing. We are not responsible for performance of the Enterprise Mobility Managed service in relation to any non-approved applications (including any User installed applications), functions and Enterprise Mobility Managed services.

Supported BlackBerry Handset Applications

Supported BlackBerry Handset Applications

Part K – Enterprise Mobility Management

1.	BlackBerry Handset **Operating System** v4.5 or later
2.	BlackBerry Handset **Address Book** Application and Settings
3.	BlackBerry Handset **Alarm** Application
4.	BlackBerry Handset **BlackBerry Messenger** Application and Settings
5.	BlackBerry Bluetooth Application
6.	BlackBerry Handset **Browser** Application and Settings – BlackBerry and Internet Browser Configurations Only
7.	BlackBerry Handset **Calculator** Application
8.	BlackBerry Handset **Calendar** Application and Settings
9.	BlackBerry Handset **Camera** Application and Settings
10.	BlackBerry Certificate Search Application
11.	BlackBerry Handset **Documents to Go** Application – v4.5 Firmware or later
12.	BlackBerry Handset **Enterprise Activation** Application and Settings
13.	BlackBerry Handset **Desktop and Folder Management**
14.	BlackBerry Handset **Help** Application
15.	BlackBerry Handset **Manage Connections** Application –devices running v4.5 or later Firmware
16.	BlackBerry Handset **Media** Application and Settings – includes Music, Videos, Ringtones, Camera, and Voice Notes folders
17.	BlackBerry Handset **Memo** Application and Settings
18.	BlackBerry Handset **Messages** Application (Enterprise Messaging) and Settings
19.	BlackBerry Messenger Application
20.	BlackBerry Network Connections (including WiFi) Application
21.	BlackBerry Handset **Password Keeper** Application
22.	BlackBerry Handset **Options** – including menu items within Options
23.	BlackBerry Handset **Phone / Call Log** Application and Settings
24.	BlackBerry Handset **Profiles** Application and Settings
25.	BlackBerry Handset **Search** Application
26.	BlackBerry Handset **Set Up Bluetooth** Application –BlackBerry Devices running v4.5 or later Firmware
27.	BlackBerry Handset **Setup Wizard** Application and Settings
28.	BlackBerry Handset **SMS / MMS** Application and Settings
29.	BlackBerry Handset **Tasks** Application and Settings
30.	BlackBerry Handset **Voice Dialling** Application and Settings
31.	BlackBerry Handset **Voice Notes Recorder** Application

Part K – Enterprise Mobility Management

Supported BlackBerry Handset hardware functions

Supported BlackBerry Handset hardware functions	
1.	BlackBerry Handset **Network Receiver** – correct network signal and strength as indicated by symbols and settings on the device.
2.	BlackBerry Handset **Phone** function – ability to make and perform phone calls
3.	BlackBerry Handset **Camera** – ability to take photos
4.	BlackBerry Handset **Power** – battery remove and replace, charging, and AC and USB cable connections
5.	BlackBerry Handset **Buttons, Keys and Trackball**
6.	BlackBerry Handset **Screen**
7.	BlackBerry Handset **Audio / Vibrations**
8.	BlackBerry Handset **Bluetooth** connections

Supported BlackBerry Enterprise Server ("BES") Application Functions and Enterprise Mobility Managed services

Supported BlackBerry Enterprise Data Enterprise Mobility Managed services	
1.	BlackBerry Alert Service (BES)
2.	BlackBerry Attachment Service (BES)
3.	BlackBerry Controller Service (BES)
4.	BlackBerry Database Consistency Check Service (BES)
5.	BlackBerry Dispatcher Services (BES)
6.	BlackBerry IT Policy Implementation and Settings
7.	BlackBerry Manager (BES 4.1 and lower)
8.	BlackBerry MDS Connection Service (BES)
9.	BlackBerry MDS Integration Service (BES)
10.	BlackBerry Administration Service (BES 5.0)
11.	BlackBerry Messaging Agent
12.	BlackBerry Policy Service (BES)
13.	BlackBerry Router Service (BES)
14.	BlackBerry Synchronisation Service (BES)
15.	BlackBerry Monitor Service
16.	Internet Access via BlackBerry MDS Connection Service
17.	Intranet Access via the BES

18.	Wireless Calendar Synchronisation and Settings
19.	Wireless Contact Synchronisation and Settings
20.	Wireless Memo Synchronisation and Settings
21.	Wireless Email Synchronisation and Settings
22.	Wireless Task Synchronisation and Settings
23.	Wireless Message Reconciliation

Approved Telstra Applications for BlackBerry Handsets

Approved Telstra Applications	
1.	Yellow Pages
2.	Where-is
3.	Foxtel

Supported BES Platform Applications

Supported Platform Applications	
1.	BES v4.1.7 to the latest RIM certified production release version
2.	Blackberry Monitor
3.	Microsoft SQL Server 2000 and 2005 versions as supported by RIM
4.	Windows Server Operating Systems versions as supported by RIM

Supported EMP Applications

Supported Enterprise Mobility Platform Applications	
1.	Good Mobile Messaging 6.0.3 or later and Mobile Control Centre 1.0.3 or later and Good Client 1.6.x or later
2.	MobileIron Advanced Management Platform
3.	Microsoft SQL Database Servers
4.	Windows Server Operating Systems
5.	AirWatch Mobile Device Management Software
6.	CellCast Solution Software

Supported EMP Applications and Functions

Supported Enterprise Mobility Platform Applications and Functions

1.	Enterprise Mobility Managed services for Corporate Wireless Email Synchronisation
2.	Enterprise Mobility Managed services for Corporate Wireless Address Book Synchronisation
3.	Enterprise Mobility Managed services for Corporate Wireless Calendar Synchronisation
4.	Enterprise Mobility Managed services for Corporate Wireless Task Synchronisation
5.	Enterprise Mobility Managed services for Corporate Wireless Memo Synchronisation
6.	Enterprise Mobility Managed services for Browsing the Internet via Enterprise Mobility Platform (EMP) Enterprise Mobility Managed services, but not Internet Browsing via other methods, such as browsing via WAP or directly to the Internet bypassing a corporate network and associated boundary controls

Supported Smartphone Handset Applications

Supported Smartphone Handset Applications	
1.	Applications directly related to accessing Corporate Email Resources from a Supported Smartphone Handset via an Enterprise Mobility Platform handset application, e.g. Good for Enterprise
2.	Applications directly related to accessing Corporate Address Books from a Supported Smartphone Handset via an Enterprise Mobility Platform handset application, e.g. Good for Enterprise
3.	Applications directly related to accessing Corporate Calendar Resources from a Supported Smartphone Handset, e.g. Good for Enterprise
4.	Applications directly related to accessing Corporate Task Resources from a Supported Smartphone Handset via an Enterprise Mobility Platform handset application, e.g. Good for Enterprise

Supported Smartphone Handset Hardware Functions

Supported Smartphone Handset Hardware Functions	
1.	Supported Smartphone Handset Hardware functions are supported in respect to access to corporate data and approved corporate functions only.

Logon name and password

4.16 We will provide you with a logon name (**Client Number**) and password which will provide you with access to the support services and tools which form part of the Enterprise Mobility Managed service.

4.17 You are responsible for ensuring the confidentiality of any Client Number and passwords issued to you as part of the Enterprise Mobility Managed service. We will not be liable for any loss or damage that you or any other person may suffer as a result of your use of the Enterprise Mobility Managed service or from disclosing your Client Number or password.

Supported Handset support

4.18 We will provide Supported Handset support, which includes support for Incidents and Requests for the Supported Handset Applications and Supported Handset hardware functions set out in the section above entitled Supported Applications, Functions and Enterprise Mobility Managed Services.

4.19 For the purposes of Supported Handset support, the Service Desk will support the following types of Requests, which will also be classified as the following Request categories for the purpose of providing Service Assurance:

Request Type	Request Category
If you have the Premium or Premium Plus package, Application / Firmware: • installation / reinstallation / uninstallation • upgrade / downgrade • update or patch version	IMACD
User changes, being swaps from one Supported Handset to another Supported Handset	IMACD
Training requests or bookings	IMACD
How Do I…? Change a setting, perform a particular function	RFI – Request for Information

4.20 For the purposes of Supported Handset support, the Service Desk will support the following types of Incidents, which will also be classified as the following Incident categories for the purpose of providing Service Assurance:

Incident Type	Incident Category
Error or performance issue with accessory (car kit or headset) or accessory connection method such as Bluetooth	Handset
Error or performance issue with Supported Handset Application not related to Data Services	Handset
Error or performance issue with the audio, volume, vibrations or associated settings on the Supported Handset	Handset
Error or performance issue with the Keys, Buttons, or Trackball on the Supported Handset	Handset
Error or performance issue with the operating system, JVM errors, Supported Handset restarts or power offs	Handset
Error or performance issue with the phone or call log functions on the Supported Handset	Handset

Physical damage with the Supported Handset – water damage, casing cracked, screen cracked	Handset
Error or performance issue with the power, charging or battery functions on the Supported Handset	Handset
Error or performance issue with profile setup and settings, custom settings and options on the Supported Handset	Handset
Error or performance issue with the device screen, backlight, screen settings on the Supported Handset	Handset

Enterprise Mobility Data service support

4.21 We will provide Enterprise Mobility Data service support, which includes support for Incidents and Requests for the Supported EMP Application Functions and services set out in the section above entitled Supported Applications, Functions and Enterprise Mobility Managed Services and provided by an EMP to a Supported Handset.

4.22 For the purposes of Enterprise Mobility Data service support, the Service Desk will support the following types of Requests, which will also be classified as the following Request categories for the purpose of providing Service Assurance:

Request Type	Request Category
Add a User to the EMP – provision Enterprise Mobility Data service on EMP. If you have the Premium Plus package: • procure and deliver the Supported Handset and SIM card (including any compatible car charger, travel kit and holster (**Starter Kit**) • porting of mobile numbers from one SIM card to another SIM card • provision the required voice and data services on a SIM card (including global roaming)	IMACD
Change a User's Account setting on the EMP: • Group • EMP Account settings – PIM Sync, Redirection	IMACD
Delete or Remove a User from the EMP If you have the Premium Plus package, deactivation of the Supported Handset and SIM card and disposal of the Supported Handset.	IMACD

License key changes: • Add CALS / SRP Key(s) • Remove CALS / SRP Key(s)	IMACD
Reset device password on the Supported Handset	Security
Reactivate device	Security
Disable device (wipe Handset)	Security
Create, Change or Delete an IT / User policy or IT / User policy setting	Security
How Do I? Change a setting, perform a particular function	RFI – Request for Information

4.23 For the purposes of Enterprise Mobility Data service support, the Service Desk will support the following types of Service Incidents, which will also be classified as the following Service Incident categories for the purpose of providing Service Assurance:

Incident Type	Incident Category
An error or performance issue with address book synchronisation	Data Services
An error or issue performance with an approved Application	Data Services
An error or performance issue with an EMP Application or service: • Service Name • BES Manager • Domino Service / MAPI Profile	Data Services
An error or performance issue with EMP infrastructure: • Mail Server • BES Server Platform	Data Services
An error or performance issue with EMP licensing: • CALS Expired • SRP Disabled / Expired	Data Services
An error or performance issue with the Browser Service: • Single Site access • Internet access • Intranet access	Data Services
An error or performance issue with calendar synchronisation	Data Services

An error or performance issue with email synchronisation: • Unable to Receive / Send • Synchronisation • Reconciliation	Data Services
An error or performance issue with instant messaging	Data Services
An error or performance issue with memos / tasks synchronisation	Data Services

4.24 When reporting an Incident or making a Request to the Service Desk you must provide all the information we reasonably require (including completing any service request forms), otherwise we may not be able to resolve the Incident or complete the Request.

Service Assurance

4.25 We will aim, but do not guarantee, to provide the Enterprise Mobility Managed service in accordance with the service levels set out below.

Service Desk

4.26 **Entry Level and Base Package – Service Desk:** We will operate a service desk for members of your company's IT department staff who have previously registered with us to contact as follows:

Enterprise Mobility Managed service package	Enterprise Mobility Managed service period	Australian Eastern Standard Time (AEST) or Australian Daylight Savings Time (ADSL)
Entry Level package	Business Hours	08:30 – 17:30 Monday to Friday (excluding National Public Holidays)
Base package	Business Hours	08:30 – 17:30 Monday to Friday (excluding National Public Holidays)
	Out Of Business Hours	20:00 – 08:00 Monday to Saturday; 08:00 Saturday – 08:00 Monday; and National Public Holidays (24 hours)

4.27 **Premium, Premium Plus Packages – Service Desk:** For all Enterprise Mobility Managed service packages except for Entry Level and Base package, we will operate a service desk for Users to contact (Service Desk) as follows:

Part K – Enterprise Mobility Management

Enterprise Mobility Managed service package	Enterprise Mobility Managed service period	Australian Eastern Standard Time (AEST) or Australian Daylight Savings Time (ADSL)
Premium package	Business Hours	08:00 – 20:00 Monday to Friday (excluding National Public Holidays)
	Out of Business Hours	20:00 – 08:00 Monday to Saturday; 08:00 Saturday – 08:00 Monday; and National Public Holidays (24 hours)
Premium Plus package	Business Hours	08:00 – 20:00 Monday to Friday (excluding National Public Holidays)
	Out of Business Hours	20:00 – 08:00 Monday to Saturday; 08:00 Saturday – 08:00 Monday; and National Public Holidays (24 hours)

4.28 Users must contact the Service Desk for all Requests, Incidents and other support in relation to the Enterprise Mobility Managed service by calling 1800 994 905 or emailing support@mscmobility.com.au (or such other phone number or email address as notified by us from time to time) during the applicable Enterprise Mobility Managed service period.

4.29 All calls and emails to the Service Desk will be classified as a Request or Incident in accordance with the sections above entitled Supported Handset support and Enterprise Mobility Data service support.

4.30 If you have the Entry Level and Base package, all calls and emails to the Service Desk which are logged outside Business Hours will be followed up by the Service Desk the next Business Day during Business Hours.

4.31 If you have the Base, Premium or Premium Plus package, a User may contact the Service Desk during Out of Business Hours for any Requests or, Incidents in relation to:

(a) Supported Handset support – but only for Requests in relation to Supported Handset passwords and Supported Handset disablement (for lost or stolen Supported Handsets); and

(b) BES or EMP Incident support – but only for platform Application monitoring and alert response / resolution.

(c) The call will be answered by an on-call service and routed to an After Hours Support Engineer who will attempt to contact the User within 1 hour of receiving the call. All calls and emails to the Service Desk which are logged during Out of Business Hours will be followed up by the Service Desk the next Business Day

during Business Hours.

4.32 If the Service Desk is unable to satisfy the Request or resolve the Incident, it may liaise with any relevant third party suppliers to complete the Request or resolve the Incident on your behalf.

Availability Targets

4.33 We will aim, but do not guarantee, to make the Service Desk available in accordance with the following availability targets:

Description	Definition	Target
Enterprise Mobility Managed service Desk Availability	Service Desk Operational Integrity including systems and process.	99%
EMP Application Availability – Hosted by you (subject to your hardware and network availability)	EMP technology functions including mail routing, 'push' functionality, user management and authentication/authorisation etc.	Base package: 97% during Business Hours. Premium package: 97%.
EMP Application Availability – Turn-Key Hosting by us	EMP technology functions including mail routing, 'push' functionality, user management and authentication/authorisation etc.	Single EMP Server: 97%. EMP Server with warm standby EMP server: 98%. EMP Server pair(s) with Active / Passive LAN Failover: 99%.

Note: EMP service availability is only applicable if we are able to deploy an EMP monitoring and alerting service.

For the avoidance of doubt, the availability target "EMP Application Availability – Turn-Key Hosting by us" described above is not limited or reduced in any way by the "Request – Response and Restoration Targets" below.

Availability in a month is calculated as the number of hours for which the Enterprise Mobility Managed service is available in that month, in accordance with the following formula:

((Scheduled Time - (Downtime - Excusable Downtime)) x 100)/ Scheduled Time

Where:

"Availability" means the Enterprise Mobility Managed service can be accessed or used by one or more Users.

"Scheduled Time" in a month means the number of hours specified as hours during which the Enterprise Mobility Managed service is scheduled to be available.

"Downtime" means the number of hours during Scheduled Time in that month during which the Enterprise Mobility Managed service is not available.

"Excusable Downtime" is any scheduled maintenance or planned outage period; any unavailability of the Enterprise Mobility Managed service caused by a defect, error or malfunction in any item of hardware, software, configuration or service, and communications not within our control; and any unavailability of the Enterprise Mobility Managed service caused by an event beyond our reasonable control.

Incident - Response and Restoration Targets

4.34 We will aim, but do not guarantee, to respond and restore an Incident within the following target timeframes:

Base package

Severity level	Response Times	Update Frequency	Restoration Times	Target
1 (Critical)	30 min	2 hour	4 hours	90%
2 (Major)	60 min	4 hours	1 Business Day	90%
3 (Minor)	2 hour	8 hours	3 Business Days	90%

Premium package

Severity level	Response Times	Update Frequency	Restoration Times	Target
1 (Critical)	15 min	1 hour	2 hours	90%
2 (Major)	30 min	2 hours	8 hours	90%
3 (Minor)	1 hour	8 hours	2 Business Days	90%

Premium Plus package

Severity level	Response Times	Update Frequency	Restoration Times	Target
1 (Critical)	15 min	1 hour	2 hours	90%
2 (Major)	30 min	2 hours	8 hours	90%
3 (Minor)	1 hour	8 hours	2 Business Days	90%

Request – Response and Restoration Targets

4.35 We will aim, but do not guarantee, to respond and restore Requests from a User (or an authorised third party) for information or advice within the following target timeframes:

Base package

Request Type	Description	Response	Restoration			Availability	
			Urgent	Standard	Target	Business Hours	After Hours
MAC	User or Device Add/Change/ Delete	2 hour	N/A	2 Business Days	90%	Yes	No
Security	Kill Pill/ Password Reset	1 hour*	N/A	1 hour	90%	Yes	No
How To / RFI	Information Request	4 hours	N/A	5 Business Days	90%	Yes	No

* Security changes will be picked up next Business Day.

Premium package

Request Type	Description	Response	Restoration			Availability	
			Urgent	Standard	Target	Business Hours	After Hours
MAC	User or Device Add/Change/ Delete	1 hour	1 hour	1 Business Day	90%	Yes	No
Security	Kill Pill/ Password Reset	15 mins**	15mins	30mins	90%	Yes	Yes
How To / RFI	Information Request	1 hour	N/A	3 Business Days	90%	Yes	No

** Response time for Security changes will be within 30 minutes after business hours.

Premium Plus package

Request Type	Description	Response	Restoration			Availability	
			Urgent	Standard	Target	Business Hours	After Hours
IMACD	Installation/Move/Change	1 hour	1 hour	1 Business Day	90%	Yes	No

IMACD	Add and Provision/Delete and Dispose/Refresh Handsets	1 hour	N/A	2 Business Days	90%	Yes	No
Security	Kill Pill/ Password Reset	15 mins**	15mins	30mins	90%	Yes	Yes
How To / RFI	Information Request	1 hour	N/A	3 Business Days	90%	Yes	No

** Response time for Security changes will be within 30 minutes after business hours.

Quality Targets

4.36 We will aim, but do not guarantee, to meet the following Quality targets in relation to the Service desk:

Base package

Metric	Target
Average Mean Time to Resolution	< 10hrs
GoS - % of calls answered with in 45 secs	70%
Abandoned calls	< 5%
Average Call Handling Time	< 15mins

Premium package

Metric	Target
Average Mean Time to Resolution	< 6hrs
GoS - % of calls answered with in 30 secs	80%
Abandoned calls	< 3%
Average Call Handling Time	< 10mins

Premium Plus package

Metric	Target
Average Mean Time to Resolution	< 6hrs
GoS - % of calls answered with in 30 secs	80%
Abandoned calls	< 3%
Average Call Handling Time	< 10mins

Part K – Enterprise Mobility Management

Note:
Mean Time to Resolution is measured as an average for all Incidents and Requests. GoS, Abandoned calls and Average Call Handling Time is measured for each inbound phone, not per User.

The above Quality targets are not included in any monthly reporting. If requested, we can provide statistics on these metrics.

Service Assurance terms

4.37 You must provide us with all reasonable assistance in a timeframe which will enable us to meet the Service Level targets. If you are unable to do so, then the applicable target timeframes will be extended by the amount of time which elapses before you are able to provide the necessary assistance.

4.38 We will not be responsible for a failure to meet any Service Level targets where the failure is caused or contributed to by:

(a) your infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed service;

(b) any unauthorised changes to your technology infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed service; or

(c) an act beyond our reasonable control.

4.39 The following statuses for Incidents and Requests will stop the Service Level clock on a ticket due to an act beyond our reasonable control to continue to resolve the Incident or Request within the applicable Service Level target:

(a) **Waiting for User** – a User has been asked to perform a test or provide feedback on a reported Incident or Request and is not able to immediately provide the feedback or perform the test. The ticket will be placed on this status which stops the Enterprise Mobility Managed Service Level clock. The Enterprise Mobility Managed service Desk will conduct an outbound follow up via phone or email with the User every 2 days to solicit the feedback and change the ticket status back to **Open** once the feedback has been received.

(b) **With Third Party –** a third party support group is required to perform an action to assist implementation of the Restore or Resolution of the Enterprise Mobility Managed service. The ticket will be placed on this status which stops the Service

Level clock. The Service Desk will conduct an outbound follow up via phone or email with the third party every day to solicit the feedback and change the ticket status back to **Open** once the feedback has been received. Where external suppliers or your infrastructure is influencing a delay in Restoration, the Restoration time will increase to the extent of the delay.

(c) **Restore-Confirm** – the Enterprise Mobility Managed service has been restored for the User but feedback from the User to confirm the Restore was successful is not immediately available. The ticket will be placed on this status which stops the Service Level clock. The Service Desk will conduct an outbound follow up via phone or email with the User every 2 days to solicit the feedback and change the ticket status back to **Open** once the feedback has been received.

Scheduled Maintenance

4.40 From time to time we will perform scheduled maintenance in connection with the Enterprise Mobility Managed service, which may involve us interrupting the Enterprise Mobility Managed service to perform work such as network upgrades, hardware / software modifications or testing. We will provide you with reasonable prior notice.

4.41 You acknowledge that during any scheduled maintenance period you may not be able to retrieve or send email, appointments, data or use other Enterprise Mobility related functions.

4.42 The Service Level targets will not apply in relation to any scheduled maintenance.

Enterprise Mobility Asset and Fleet Management (Supported Handset pool)

4.43 If you have the Premium Plus package, we will:

(a) establish and manage a Supported Handset pool for the purpose of replacing faulty Supported Handsets and provisioning new Supported Handsets;

(b) track and record required Enterprise Mobility asset details for all your Users;

(c) report on required Enterprise Mobility asset details for asset management purposes; and

(d) make recommendations on refreshing your Supported Handsets where they are 24 or more months old from the date or purchase and/or based on our assessment on the reliability and serviceability of the Supported Handset.

4.44 We will keep the Supported Handset pool at a minimum level of 3% of your total

Supported Handset fleet, provided there are no restrictions on the supply of Supported Handsets from Supported Vendors.

4.45 You must notify us of any change in the size of your Supported Handset fleet which is greater than 10%, in which case the parties will discuss and agree any necessary changes to the Enterprise Mobility Managed service.

4.46 We will not be responsible for any Supported Handset which is not under our direct control.

EMP Platform Application - Maintenance and Monitoring

Capacity Management – Monthly User Licence

4.47 We will perform capacity checks for active and inactive Users against your client access licence levels.

4.48 We will provide a monthly report that contains:

(a) Number of inactive (not activated / not running) Users;

(b) Users who have had no contact with the EMP for more than 14 days; and

(c) Users who have had no contact with the EMP for more than 28 days.

Availability Management – EMP service monitoring

4.49 We will monitor the Supported EMP Application functions and services set out above in the table under the heading “Supported EMP Application and Functions” for continuous stoppages of more than 5 minutes, and will generate an alert for each event of this kind. Each alert is generated as an Incident and will be initially logged as a Severity 3 Incident while we conduct further investigations. We will raise the Severity Level upon repeat alerts or if our investigations determine it is a Severity 1 or 2 Incident.

4.50 Some or all of the following EMP services may be necessary for consistent performance of the EMP core solution functions such as Email and Organiser Data Synchronisation and Reconciliation:

(a) EMP Alert Service;

(b) EMP Attachment Service;

(c) EMP Collaboration Service (Enterprise Instant Messaging Integration only);

(d) EMP Controller Service;

(e) EMP Dispatcher Service;

(f) EMP Mobile Access or Connection Service (Internet Browsing);

(g) EMP Policy Service;

(h) EMP Router Service; and

(i) EMP Synchronisation Service.

Self-service monitoring

4.51 As part of the Enterprise Mobility Managed service we will provide you with the ability to measure the connection status of the Messaging Agent (the Enterprise Mobility service that scans a User's mailboxes and assists with synchronising changes to the User's Supported Handset) via a simple customised Windows Performance Monitor.

4.52 To maximise the availability of your Enterprise Mobility Managed service, we recommend you regularly:

(a) perform Database consistency checks to ensure that the Enterprise Mobility Configuration Database (which is the core of the Enterprise Mobility solution and contains your Users' device settings and configuration data) remains stable and avoids corrupted data; and

(b) create an automated ticket to log a Request in relation to each Database consistency check performed in accordance with paragraph (a) above to confirm whether the check was successful or unsuccessful.

Release Management

4.53 We will review each EMP deployment of either an application or a release, upgrade, update or patch (in relation to your EMP service or Supported Handset) that has been issued by a Supported Vendor and acquired by you from us or the Supported Vendor (**Release**) for applicability and criticality when they are available as a general release from the Supported Vendor. If we consider the Release to be relevant to maintaining the availability and security of your EMP service, and provided it does not impact functionality, we will:

(a) if you have the Base package, test and implement the Release (for EMP software and select updates only) within 90 days of the Supported Vendor making it

available as a general release; and

(b) if you have the Premium or Premium Plus package:

(i) test and implement each major EMP Release within 90 days of the Supported Vendor making it available as a general release;

(ii) test and implement each minor EMP Release within 60 days of the Supported Vendor making it available as a general release; and

(iii) implement any Supported Handset firmware upgrades and/or patching, either prior to Supported Handset activation or at the recommendation of the Supported Vendor,

in accordance with the change and release management process set out in the section under the heading Change and Release Management Process below.

Change and Release Management Process

4.54 You must notify us of any planned changes to the platform and its services, including the operating system, back-ups, anti-virus and security as follows:

(a) for regular changes, you must provide us with at least 14 days prior notice; and

(b) for emergency changes, you must provide us with at least 8 Business Hours' notice.

4.55 Each change or release, including changes to the EMP configuration, must be approved by the parties before it is implemented. We will not approve a change until the following actions have been satisfied:

(a) change definition completed;

(b) change windows identified, including resource availability (physical and technical);

(c) change tasks defined;

(d) roll-back tasks defined;

(e) test plan defined;

(f) test plan actioned, including roll-back plan (subject to constraints notified by us);

(g) change window confirmed (release date);

(h) Enterprise Mobility Managed service Desk notified of release date;

(i) you have informed us that internal approval has been provided by each of your internal representatives concerned with the change; and

(j) each of our representatives and specialists has approved the change.

4.56 You must not make any changes to the infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed service without complying with the section above under the heading Change and Release Management Process. You indemnify us against all losses suffered or incurred by us arising out of or in connection with your failure to comply with the section above under the heading Change and Release Management Process.

Service Management

Enterprise Mobility Managed service reports

4.57 If you have the Base package, we will provide the following monthly reports:

(a) a ticket list report that contains the following information in relation to all Incidents and Requests logged by the Service Desk:

(i) Date logged;

(ii) Ticket Reference;

(iii) Ticket Category and Type;

(iv) Summary of ticket details;

(v) Resolution Summary;

(vi) Service Level timestamps; and

(vii) Resolution time.

(b) a simple maintenance report of the EMP Applications that contains the following information:

(i) EMP Application licence levels (being the total available client access licence and total number of Users);

(ii) changes to EMP infrastructure and environment; and

(iii) any other recommendations (on a quarterly basis) on improving the Enterprise Mobility Mobile Wireless service with respect to EMP infrastructure and applications.

4.58 If you have the Premium or Premium Plus package, we will provide the following monthly reports:

(a) a ticket list report as set out in this section above; and

(b) a Enterprise Mobility Managed service report that contains the following information:

(i) changes to EMP infrastructure and environment;

(ii) Availability;

(iii) any unplanned outages, including root cause analysis and suggested preventative measures;

(iv) Releases implemented;

(v) capacity of EMP infrastructure and Applications; and

(vi) any other recommendations on improving the Enterprise Mobility Mobile Wireless service with respect to EMP infrastructure and applications.

4.59 If you have the Premium Plus package, we will also provide a monthly Enterprise Mobility asset management report that contains the following information:

(a) Supported Handset pool levels;

(b) Number of new Supported Handsets;

(c) Number of Supported Handsets repaired and refreshed; and

(d) Forecast of Supported Handsets to be refreshed over the next three months.

Enterprise Mobility Managed service meetings

4.60 If you have the Premium Plus package, we will meet with you each month at an agreed time and place to review and discuss the monthly Enterprise Mobility Managed service report.

Law of Large Numbers

4.61 Because percentages become less accurate for displaying results the smaller the number becomes, if the total number of tickets logged for a particular category of Incident or Request is less than 40, the below table will be used to measure and display Service Level results for reporting in accordance with the section above under the heading Change and Release Management Process.

Total Number of Tickets Logged	Allowable Ticket Failures	Ticket Failures / Enterprise Mobility Managed service Level result		
		Failure to meet Enterprise Mobility Managed service Level Targets	Enterprise Mobility Managed service level Targets achieved	Enterprise Mobility Managed service Level Targets exceeded
1 to 10	1	≥ 2	1	0
11 to 20	2	≥ 3	2	≤ 1
21 to 30	3	≥ 4	3	≤ 2
31 to 40	4	≥ 5	4	≤ 3

Note: Service Level results are measured and displayed by the number of ticket failures compared to the total with an allowable number of failures per range of 10 tickets.

Fleet Management Service Level Targets (Premium Plus Package Only)

4.62 This section in relation to Fleet Management Service Level Targets applies only to Premium Plus package customers.

4.63 We will try, but do not promise, to meet the following service level targets for the following fleet management services outlined below:

Fleet Management Services	Application	Service Level Targets

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Mobile device delivery for up to 100 new service connections (For orders of mobile devices and accessories for more than 100 new service connections, this target will not apply. We will discuss and agree a delivery time with you.)	This service level target **only** applies to: • telephone and email orders from Users; and • email orders from users with Other Devices which are directed to and received at our nominated Enterprise Mobility Managed Service Desk email address.	**For delivery of 90% of new mobile devices** Provided the Enterprise Mobility Managed Service Desk receives your completed **telephone or electronic order** on a business day before 12.00pm (AEST): • Delivery to **Metropolitan** areas – next business day following receipt of your order. • Delivery to **Regional** areas – within 2 business days following receipt of your order. • Delivery to **Remote** areas - within 5 business days following receipt of your order. **Note:** There are no deliveries on weekends or public holidays. Next day delivery may not be possible in the circumstances where the mobile device model requested by you is out of stock or is not available from the manufacturer; the mobile device model requested by you has been discontinued; we are unable to deliver the mobile device to you because your delivery address is incorrect or incomplete; we are unable to gain access to your site to deliver the mobile device to you, or for any reason beyond our reasonable control.

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Faulty mobile device repairs	This service level target **only** applies to: • telephone and email orders from Users; and • email orders from users with Other Devices which are directed to and received at our nominated Enterprise Mobility Managed Service Desk email address	**For 90% of faulty mobile devices:** Repair and delivery • Spare Pool location in **Metropolitan** areas – within 11 business days from receipt of your mobile device by the Telstra Repair Centre • in all other areas – within 20 business days from receipt of your mobile device by the Telstra Repair Centre. **Note:** There are no deliveries on weekends or public holidays. This service level target does not apply if: • replacement parts are not available for your mobile device from the mobile device manufacturer; • the Enterprise Mobility Managed Service Desk determines that your mobile device needs to be returned to the mobile device manufacturer for repair.

Part K – Enterprise Mobility Management

Fleet Management Services	Application	Service Level Targets
Replacement of lost or stolen mobile devices	This service level target **only** applies to: • telephone and email orders from Users; and • electronic orders from users with Other Users Devices which are directed to and received at our nominated Enterprise Mobility Managed Service Desk email address	**For delivery of 95% of replacement mobile devices** Provided that the Enterprise Mobility Managed Service Desk receives your completed **telephone or electronic order** on a business day before 12.00pm (AEST): • Delivery to **Metropolitan** and **Regional** areas – next business day following receipt of your order. • Delivery to **Remote** areas - within 5 business days following receipt of your order. **Note**: There are no deliveries on weekends or public holidays. Delivery within the above timeframes may not be possible in the circumstances where the mobile device model requested by you is out of stock or is not available from the manufacturer; the mobile device model requested by you has been discontinued; we are unable to deliver the mobile device to you because your delivery address is incorrect or incomplete; we are unable to gain access to your site to deliver the mobile device to you, or for any reason beyond our reasonable control.

4.64 The above service level targets will not apply:

(a) if you order mobile devices, services or activations through any delivery channel other than the Enterprise Mobility Managed Service Desk; or

(b) to any orders received in relation to Other Users Devices (as described in clause above under the heading "Eligibility").

Additional Services

4.65 For an additional fee, you may also purchase additional services in the form of:

(a) 24/7 Service Support;

(b) Managed App Services (**MAS**); and

(c) Managed App Reputation Scanning (**MARS**),

together the (**Additional Services**).

4.66 The Additional Services are only available to Customers with an existing EMMS service (which may include T-MDM or supported MDM).

24/7 Service Support

4.67 We will operate a 24 hour, seven day a week service desk (24/7 Service Support) for your company's staff to contact which includes the full capabilities of the Service Desk but on a 24/7 operational cycle and is available for all Enterprise Mobility Managed service packages.

4.68 Users must contact 24/7 Service Support for all Requests, Incidents and other support in relation to the relevant Enterprise Mobility Managed service by calling 1800 994 905 or emailing support@mscmobility.com.au (or such other phone number or email address as notified by us from time to time) during the applicable Enterprise Mobility Managed service period.

4.69 All calls and emails to 24/7 Service Support will be classified as a Request or Incident in accordance with relevant clauses beginning at clause 4.34.

4.70 If 24/7 Service Support is unable to satisfy the Request or resolve the Incident, it may liaise with any relevant third party suppliers to complete the Request or resolve the Incident on your behalf.

4.71 We aim, but do not guarantee, to make 24/7 Service Support available in accordance with the Availability Targets set out in the relevant clauses beginning at clause 4.40.

4.72 For a monthly account level access fee (as set out in 4.74) the 24/7 Support Service includes the following:

Service Matrix

4.73 The 24/7 Service Support includes the following functionality:

Service Desk – General Service Access	

Part K – Enterprise Mobility Management

Email and Phone Support	Tickets can be logged with Telstra via phone or email as per the Service Desk phone number and email address respectively. It is recommended that End Users use phone support for After Business Hours (urgent / business critical incidents).
End User Service Desk – Level 1 First Point of Contact	A Level 1 Service Desk service with direct End User support. All incidents and requests are directed to Telstra who will manage resolution and escalation.
IT Service Desk Support – Level 2 and Level 3 IT Escalations	A Level 2 and 3 Service Desk for escalations from a Telstra Customer's IT service desk. All MDM administration is performed by our 3rd party.
MDM Administrator Support	A Level 3 Service Desk for Business Critical Severity 1 incidents and MDM console access incidents ONLY.
Product Vendor Escalations and Management	Product Vendor related incidents are escalated to the Product Vendor and managed by Telstra's 3rd party where required.

Service Items	**Description**	**Service Desk**		**24/7 Support Services**
		Business Hours	**After Hours**	**24/7**
		08:00 – 20:00 MF	**20:00 – 08:00 SM**	**0:00 – 23:00 SM**
Incident and Request Management				
Mobile Device Support – Incidents and Request	Support for Device Related Services and Functions	✓		✓
MDM Platform Support — MDM Configuration Requests	Function or application related to Configuration on the MDM Server (This could be a user or platform configuration on the MDM Server).	✓		
Carrier Support Escalations — Incidents and Requests	Managed escalations to your Network Carrier for SIM Card Service Requests and Incidents.	✓		✓
MDM Vendor Escalations – Incidents and Requests	Managed escalation to Product Vendors for MDM platform related queries and / or issues	✓		✓
MDM Platform Support – Incidents ONLY	Support for Business Critical Severity 1 incidents ONLY	✓	✓	✓
24/7 Mobile Device Support - Requests for Password Resets and Lost and Stolen - Data Wipe Only	Support for Password Resets and Lost or Stolen Devices ONLY	✓	✓	✓

Part K – Enterprise Mobility Management

24/7 Mobile Device Support – Incident and Service Requests for Roaming Users	Support for Roaming Users for Incidents and Requests. User MUST be travelling temporarily overseas	✓	✓	✓
Release and Change Management				
MDM Policy Breach Management	Monitoring of MDM Policy breaches on devices and management of resultant actions of policy breach	✓		✓
Release and Change Management — Patch and Maintenance Releases	Maintenance Releases and Patching are performed for the selected MDM Platform	✓		
Availability Management — Platform Service Monitoring	Platform Monitoring for Service Uptime and Unplanned Outages	✓	✓	✓
High Priority Incident Management	Support for incidents that require a higher tier support group due to the incident severity pertaining to urgency and impact	✓	✓	✓
Service Management				
Single Point of Contact Service Management	A Service Delivery Manager is assigned to your account providing a single point of contact for escalations, ad hoc business Q&A and service management tasks	✓	✓	
Monthly Service and Ticket Reporting	A Monthly Report detailing performance against Service SLA's and recommendations on improving the service	✓		
Monthly Service Review Meeting	A Monthly meeting to review the monthly report and discuss items in the service	✓		
High Priority Incident Management contact	Single point of contact coordination and stakeholder communications during High Priority Incidents (including Afterhours duty SDM)	✓	✓	✓
Continual Service Improvement	Management of process enhancements and Service Improvements Programs	✓		
Fleet Management (all service items below are optional)				

Device Procurement & Logistics	Management of Device Ordering, Fulfilment and any Logistics in relation to Device Ordering	✓		
Device Staging and Deployment	Management of the device staging and MDM enrolment processes prior to delivering to the End User	✓		
Device Repair and Replacement Management	Management of device hardware faults, repair processes, and a device spare pool for device replacements	✓		
Fleet Location Management and Tracking	Management of device to user assignments and locations of devices.	✓		
Asset Reporting	An additional section in the monthly report detailing asset (device) movements for the month	✓		

24/7 Service Support - Pricing

4.74 24/7 Support Service charges:

24/7 Service Support Components	Low	Medium	High
Per Month Access (GST Exclusive)	$2,500.00	$5,000.00	POA
Per Month Access (GST Inclusive)	$2,750.00	$5,500.00	POA
Per Ticket (GST Exclusive)	$150.00	$125.00	POA
Per Ticket (GST Inclusive)	$165.00	$137.50	POA
Fair Use Policy (FUP)*	20 tickets	50 tickets	POA

Note:

- *Fair Use Policy (FUP) – has been designed to meet the organisational requirements of Customers. This tiered pricing includes the FUP that indicates the ticket per month allowance.
- 24/7 Service Support ticket reports will be generated monthly and provided through Service Delivery Management channels.
- End User app support service consumption is reviewed monthly and adjustments are negotiated quarterly.
- This product has been developed for existing EMMS Customers but is also available to new EMMS Customers.

Managed App Services (MAS)

4.75 MAS is a suite of services incorporating app procurement, deployment, configuration, security, reporting, compliance and support. It also provides an optional capability to have a managed service wrapped around Bespoke Enterprise App Management (as set out in clause 4.85 below) for Telstra preferred app developers that can assist in the complex change management of bespoke app deployment and support.

4.76 MAS includes:

(a) Service Design, Build & Implementation (Mandatory Customer requirement)

(b) Public Business and Productivity App Matching

(c) Corporate App Store Branding & Management

(d) Corporate App Procurement Service

(e) MAS - Reporting

(f) MAS - Ongoing Maintenance and Upgrades

(g) Bespoke Enterprise App Management - Optional

Service Design, Build & Implementation (Mandatory Customer requirement)

4.77 Service Design and build process consists of an introductory meeting between you and Telstra representatives) to define and design the MAS as per your business requirements. We will manage the end to end design of the service, implement and activate the required components. The process includes the following:

(a) Project Scoping

(b) Agreed Service Design & Statement of Work

(c) Build, test, pilot & sign off

(d) Service Transition & on boarding

(e) EMMS Platform Configuration

(f) Public App Management (Optional)

Part K – Enterprise Mobility Management

Public Business and Productivity App Matching

4.78 We will consult with you to define a policy around how public apps are managed on your device fleet to understand current app usage by Users, define a list of same or equivalent apps that allow business continuity to be pushed out to Users and which can be automatically or manually updated over Wi-Fi or cellular networks.

Corporate App Store Branding & Management

4.79 Supplier will define and build a corporate branded App store as a single go to reference for End Users to retrieve recommended business and productivity apps for the End User. The corporate app store will be pushed down over the air and may incorporate the Customer's corporate logo and or colours if required (platform dependent).

Corporate App Procurement Service

4.80 We will provide an app procurement service for you to enable you to purchase and deploy paid public apps which can be licensed, billed and registered to your business. We may also assist in the integration of the app store licensing to EMMS supported platforms and push these apps over the air or remove them when required from your Users' devices (iOS Devices only).

MAS - Reporting

4.81 We will report to you monthly on applicable service level utilization and implementation which will include the following:

(a) Project Management Implementation;

(b) Apps deployed on EMMS platforms;

(c) App version information;

(d) Corporate App Store Apps;

(e) Bespoke Enterprise Managed Apps; and

(f) Paid Public App Licensing.

MAS - Ongoing Maintenance and Upgrades

4.82 We will provide ongoing maintenance of the Managed App Service including Corporate App Store Management, Procurement and Management of Apps & Public App

Management. From time to time we may also be required to undertake any underlying platform upgrades to maintain the Managed App Service.

4.83 You acknowledge that during any scheduled maintenance period you may not be able to retrieve or use apps or other Enterprise Mobility related functions.

4.84 Any Service Level targets will not apply in relation to any scheduled maintenance.

Bespoke Enterprise App Management - Optional

4.85 The Bespoke Enterprise App Management provides you with support to build and deploy enterprise apps for End Users. We provide the managed services to work with app developers to ensure that apps are deployed correctly, maintained and meet your corporate compliance standards and are effectively supported.

4.86 We will work with our preferred app developers to provide you the following:

(a) service design - build a level of service to meet your business requirements based on the supported app;

(b) secure app retrieval from the developer – we will work with the supported developer to ensure that app code is transferred in a secure method to the EMMS platform;

(c) app deployment through EMMS supported platforms - creation of group and device deployment polices (including basic testing) to User devices over the air and app updates when required within fair use policy.

(d) change & release management - manage timing of releases with the supported app developers to manage app deployment, changes and updated to software;

(e) user credentials field injection for supported apps - where supported, We can populate app settings on mass with user credentials which can significantly increase User experience;

(f) User support for Bespoke Enterprise Managed Apps - Users may call the Service Desk for bespoke Enterprise App Support for which we will endeavour to provide assistance at first call;

(g) basic app troubleshooting and escalation – We will provide basic app troubleshooting services with defined apps for Users; and

(h) ticket management for supported Bespoke Enterprise Managed Apps – where

required, we will escalate support to the app developer and manage the service ticket until close within standard SLA's as set out in clauses 4.34 and 4.35.

Managed App Services charges:

4.87 The Managed App Service charges are as follows:

Managed App Service Components	Charges (GST Exclusive)		Charges (GST Inclusive)			
Public App Management						
Service Design, setup and Implementation. Once off setup fee.	$5000.00		5,500.00			
Public App Management Service Fee - per month	$2000.00		$2,200.00			
Bespoke Enterprise App Management						
	1 - 5 Apps (GST Exclusive)	1 - 5 Apps (GST Inclusive)	6 - 10 Apps (GST Exclusive)	6 - 10 Apps (GST Inclusive)	10 + Apps, (GST Exclusive)	10 + Apps (GST Inclusive)
Bespoke Enterprise App Deployment - per app	$4000	$4,400	$4000	$4,400	POA	POA
App maintenance – per app per month (incl. 2 changes per month)	$1500	$1650	$1250	$1,375	POA	POA
Additional changes thereafter per request	$500	$550	$500	$550	POA	POA

App Support Service Consumption rates	2.00% ticket rate	.00% ticket rate	2.63% ticket rate	2.63% ticket rate	2.8% ticket rate	2.8% ticket rate
User Service Desk Support - per app, per month.*	$1.55	$1.71	$1.85	$2.04	$2.15	$2.37

Note:

- User app support measured as tickets raised per app per month as a % of each app in deployed population.
- All End User app support services start at reference rate of 2.8%.
- End user app support service consumption is reviewed monthly and adjustments are negotiated quarterly.
- End user app support service fees may be higher or lower than the listed fees if very high or very low consumption rates occur in the support trend.

Managed App Reputation Scanning (MARS) service

4.88 The MARS Service is an optional feature of the Managed App Service which is only available to EMMS Customers who have T-MDM or another supported MDM.

4.89 The MARS Service includes:

(a) Service Design, Setup & Implementation

(b) Integration & Management; and

(c) MARS Reporting and Ongoing Management

MARS Service Design, Setup & Implementation

4.90 Service Design and Setup consists of an introductory meeting with you to define and design the Managed App Reputation Scanning solution tailored to your requirements. We will manage the end to end design of the service, implementation and activate the required components which include the following:

(a) Project Scoping;

(b) Security policy design;

(c) Escalation process design and remediation rules;

(d) Agreed Service Design & Statement of Work;

(e) Build, test & sign off; and

(f) Service Transition & on boarding.

4.91 We will provide identification of apps which we believe may show signs of risky behaviour and are therefore a security or stability threat to your device fleet. We will automatically remediate them based on your business security requirements and build appropriate policy to follow in the future as well as provide regular app security updates reports.

4.92 As part of our Security Policy Design, we will develop remediation actions, policy definition, whitelisting and blacklisting of apps to maintain security standards taking into account a balance between risk and your users' experience.

MARS Integration & Management

4.93 EMMS & App Reputation Scanning Integration: We will integrate the cloud hosted App Reputation Scanning engine with the existing EMMS platform (including where you who have selected T-MDM or other supported platform as your MDM platform) which requires the installation and configuration of the scanning engine with the MDM platform for reporting.

4.94 The App Reputation Scanning Engine hosting is included in the Managed App Service.

MARS Reporting and Ongoing Management

4.95 Reporting: We will provide monthly reporting in discussion with you around app risk analysis which will be delivered through service management by performing the following:

(a) Devices scanned & under management;

(b) Unique apps in the device environment;

(c) App risk violations report;

(d) Top 10 riskiest apps;

(e) Policy violation intelligence;

(f) Risk reduction intelligence;

(g) Policy management; and

(h) Tailored compliance remediation review.

4.96 Ongoing Management and Maintenance: As a part of our ongoing maintenance of the Managed App Reputation Scanning Service, We will maintain the MARS service for you which includes app scanning, updates, integration and policy management and we will ensure that any underlying platform upgrades are performed to maintain the Managed App Reputation Scanning Service.

Managed App Reputation Scanning - Pricing

4.97 The following charges apply for the Managed App Reputation Scanning service:

Managed App Reputation Scanning Service			
Volume	5000	5001-10,000	10,000+
Service Design, setup and Implementation. Once off setup fee. **(GST Exclusive)**	$10,000	$10,000	POA
Service Design, setup and Implementation. Once off setup fee. **(GST Inclusive)**	$11,000	$11,000	POA
Monthly Service Fee per Supported Device **(GST Exclusive)**	$2.50	$2.00	POA
Monthly Service Fee per Supported Device **(GST Inclusive)**	$2.75	$2.20	POA

MARS Minimum Term

4.98 If you take up MARS as part of your Enterprise Mobility Managed Service 2 on or after 20 November 2016, you must do so for a minimum term of 12 months (MARS Minimum Term). If your Enterprise Mobility Managed Service 2 or MARS is cancelled or terminated during the MARS Minimum Term other than for our breach your agreement with us, early termination charges (MARS ETCs) will apply for MARS.

The ETC will be calculated as follows:

A x B x C x 0.75= ETC

where,
A is the applicable Monthly Service Fee per Supported Device for your MARS;
B is your number of Supported Devices; and
C is the number of months remaining (or part thereof) of the MARS Minimum Term.

Other professional services

4.99 If requested we can provide other professional services. We will provide you with a quote for your approval before providing any other professional services.

Your obligations

4.100 You must nominate a person to be your single point of contact with us for all matters in relation to the Enterprise Mobility Managed service.

4.101 Unless otherwise specified as part of your Enterprise Mobility Managed service package, you and your Users are responsible for the purchase of any Enterprise Mobility service, Supported Handsets and accessories, and any other ancillary products and services.

4.102 Unless we host the Enterprise Mobility Platform, you must not prevent us from connecting to the EMP server located on your premises for the purpose of us providing the Enterprise Mobility Managed service, unless the method of connection:

(a) breaches your documented IT security policy for remote connections;

(b) poses a significant and tangible threat to your business operations; or

(c) your Enterprise Mobility Managed service has been terminated.

4.103 You acknowledge that mechanisms and procedures that you may use for the purpose of establishing secure external third party connections may hinder or prevent us from providing the Enterprise Mobility Managed service. If so, the parties will work together in good faith to implement a suitable external third party connection scheme that will enable us to provide the Enterprise Mobility Managed service.

4.104 You:

(a) must not resell or resupply the Enterprise Mobility Managed service;

(b) unless we host the Enterprise Mobility Platform, are responsible for the platform and its services including the operating system, back-ups, anti-virus and security. Backups should include the SQL database, Applications and the operating system;

(c) must not make any unauthorised changes to any infrastructure, software (including email systems) or configurations that support the Enterprise Mobility Managed service without complying with the change and release management process set out in the section under the heading Change and Release Management

Process above;

(d) must notify us of any changes to your technology environment which may impact the Enterprise Mobility Managed service, including any changes to your email infrastructure and network (such as firewalls and gateways);

(e) provide us (or our representatives) with all reasonable assistance and access to your information, premises and systems as requested by us from time to time in connection with us providing the Enterprise Mobility Managed service; and

(f) comply with all our reasonable instructions and procedures in relation to the Enterprise Mobility Managed service as notified to you.

4.105 You must ensure that you have sufficient security infrastructure in place to prevent email viruses, denial of service attacks and other malicious digital attacks. We will not be liable for any loss or damage that you or any other person may suffer as a result of:

(a) your Supported Handsets; or

(b) unless we host the Enterprise Mobility Platform, EMP infrastructure,

(c) becoming infected with a virus, malware or other form of malicious software.

4.106 If we need to attend your premises in relation to the Enterprise Mobility Managed service, you must ensure that our personnel (or our representatives) are provided with a safe and appropriate working environment when working on your premises.

4.107 You warrant that your use of the Enterprise Mobility Managed service will not:

(a) breach any law, regulation, industry code or standard; or

(b) infringe the rights of any third party.

4.108 You indemnify us against all losses suffered or incurred by us arising out of or in connection with your failure to comply with this section entitled “Your Obligations” .

Using your handset overseas

4.109 You could breach the laws of another country (in particular the United States or Canada) if you use, send or take a handset outside of Australia. This is partly due to laws regulating the importation, exportation and use of encryption software contained within a handset.

4.110 You may only use the handset in, or send or take it to or from, other countries approved by us for your network. We will provide a list of approved countries for handset on the telstra.com website. We may update this list from time to time.

Password protection

4.111 Each Supported Handset has a password protection function. You must make sure that this function is always activated on your Supported Handset, regardless of who is using it.

Responsibility for use of the Enterprise Mobility Managed service

4.112 You are solely responsible for your use of the Enterprise Mobility Managed service and the content and security of any data or information which is sent or received using your Supported Handset and the Enterprise Mobility Managed service.

General

4.113 You must use your Supported Handset, our services and our networks in accordance with our Acceptable Use Policy available www.telstra.com. We may terminate your access to our networks if you use them to adversely impact the operation and/or other customers' enjoyment of our network or if you breach a material term of these terms, in accordance with the General Terms of Our Customer Terms (to see these terms – home and family customers click here; business and government customers click here). We will tell you before this happens.

Special Meanings

4.114 The following words have the following special meanings:

(a) **Enterprise Mobility Platform** or **EMP** means the component of the Enterprise Mobility Managed service solution that either provides corporate wireless data synchronisation and device management services to Supported Handsets, or manages the corporate wireless data synchronisation and device management services to Supported Handsets. The enterprise mobility platform is made up of server infrastructure, an operating system and an enterprise mobility platform application.

(b) **Incident** means an event which is not part of the standard operation of a service and which causes or may cause disruption to a reduction in the quality of services and User productivity, as described in the sections above entitled Supported Handset support and Enterprise Mobility Data service support.

(c) **Metropolitan Area or Metropolitan** means the metropolitan areas of the

following cities:

(i) Sydney,

(ii) Canberra,

(iii) Melbourne,

(iv) Hobart,

(v) Adelaide,

(vi) Brisbane,

(vii) Perth,

(d) **Request** means a request from a User (or an authorised third party) for information or advice, as described in the sections above entitled Supported Handset support and Enterprise Mobility Data service support.

(e) **Response** occurs when action is taken to assign an Incident or Request ticket and an email is sent to the requestor to inform them the Incident or Request has been received and assigned to an individual person for resolution.

(f) **Restoration** occurs when action is taken to implement and confirm that the User has the required level of Enterprise Mobility Managed service working to perform their job role or function (E.g. restore an email sending incident so the User can send email from their Supported Handset). Restoration may be implemented by performing a workaround or temporary resolution which will be followed up at a later date and have a permanent resolution implemented or may be implemented using a permanent resolution.

(g) **Severity 1 (Critical)** means failure of the system with a major business impact affecting more than one User, business critical system or process with no workaround.

(h) **Severity 2 (Major)** means one or more Users are affected by the failure of a business critical system or Application which may have a workaround that cannot be sustained over a reasonable period of time (more than 1 day).

(i) **Severity 3 (Minor)** means one User is affected and not business critical which may have a workaround that can be sustained over a reasonable period of time

(more than 1 day).

(j) **Standard Request** means there is no immediate impact and the request is not business critical.

(k) **Supported Handset** means:

(i) an eligible BlackBerry handset that is manufactured by Research in Motion Limited (**RIM**) and approved by us, including the BlackBerry 81XX, BlackBerry 8800, BlackBerry Bold 9XXX, BlackBerry Curve and BlackBerry 87XX models; and

(ii) an eligible smartphone handset that is manufactured by a Supported Vendor and approved by us, including the Apple iPhone MC131X or later model, Apple devices running iOS 3.1 or later version, devices using the Windows Phone 7 operating system, and devices using the Android operating system.

(l) **Supported EMP Vendor** means a vendor that supplies Enterprise Mobility Platform services that are approved by us and compatible with the Enterprise Mobility Managed service. Our list of Supported EMP Vendors may change from time to time. You may request a copy of our list of Supported EMP Vendors at any time.

(m) **Supported Vendor** means a vendor that manufactures smartphones or other mobile handsets and that is approved by us, including Apple Pty Limited and Apple Inc. Our list of Supported Vendors may change from time to time. You may request a copy of our list of Supported Vendors at any time.

(n) **Urgent Request** means there is an immediate impact and / or the request is business critical.

5 Telstra Mobile Device Management ("T-MDM") service

PART A – Terms and conditions for your T-MDM service

5.1 The Telstra Mobile Device Management ("T-MDM") service is a hosted platform that allows you to manage mobile devices running a compatible operating system listed at www.telstra.com/enterpriseclassdevices that have an active internet connection (either Wi-Fi or mobile coverage) (“Compatible Devices”).

5.2 Your nominated representative(s) can access your T-MDM platform on the internet and register your employees and contractors that have a Compatible Device ("**End Users**") so

that your company policies, settings and applications are pushed to those Compatible Devices. End Users have to opt-in and setup their Compatible Device(s) by entering a set of credentials provided by you before company settings are pushed.

Eligibility

5.3 To be eligible to take up the T-MDM service, you must have:

(a) an ABN, ACN or ARBN; and

(b) one or more Compatible Devices,

(c) ("Eligible Customer").

T-MDM platforms

5.4 When you take up a T-MDM service, you can choose between two different T-MDM platforms:

(a) a shared platform powered by AirWatch ("**T-MDM Shared Platform**"); or

(b) a dedicated platform powered by Citrix ("**T-MDM Dedicated Platform**").

5.5 The features of the T-MDM Shared Platform and T-MDM Dedicated Platform are set out in the table below.

Feature	Description	T-MDM Shared Platform	T-MDM Dedicated Platform
Minimum number of registered Compatible Devices		1	300 minimum
Hosting Location		Telstra Cloud, Australia	Amazon Web Services, Australia
Platform Upgrades	How platform upgrades occur	Software upgrades are automatically applied with 5 days' notice	You notify Telstra when upgrades should take place based on your change management window
Mobile Device Management	Protect company information on Compatible Devices by configuring IT policies	Included	Included

Part K – Enterprise Mobility Management

Feature	Description	T-MDM Shared Platform	T-MDM Dedicated Platform
Mobile Application Management (MAM)	Create an enterprise application store and manage applications on Compatible Devices	Included	Included
Mobile Content Management (MCM)	Upload and share company documents and collaborate with colleagues	Basic functionality	Included
Mobile Email Management (MEM)	Control which Compatible Devices have email access and encrypt email messages	Included	Included
Unlimited SMS	No charge for sending SMS messages to Compatible Devices registered on a T-MDM platform	Included	Included
Digital Forms	Digitise paper based forms onto tablets and smartphones	Not available	Included
Zimperium Intrusion Protection Solution (zIPS)	An app that protects devices from malware and network security threats	Included	Included
Device Enrolment Service (DES)	Deploy devices ready to go out of the box with company settings and apps	Included	Included
Cloud Storage	Storage provided by Telstra to upload company documents	25GB include	Not available
Integration with enterprise resources	Ability to connect with enterprise systems like Active Directory, share file, per app VPN, etc.	Included (requires software adapters installed in your premise (installed at an additional cost))	Included (requires an IPSec VPN appliance installed in your premise (installed at an additional cost))

Feature	Description	T-MDM Shared Platform	T-MDM Dedicated Platform
Telstra Managed Mobiles Solution Service	Enhanced service management and support throughout Australia for eligible services.	Additional cost	Additional cost

5.6 End Users may be required to install third party software on their Compatible Devices to be able to use the T-MDM platform. The third party software vendors may impose additional terms on the use of that software, and you and your End Users must agree to those terms.

Sign-up process

5.7 To access your T-MDM platform, you will have to complete and sign a 30 day trial online application form with a nominated Telstra mobile account number. We will only provide the login to your nominated representatives(s). If we ask you to, you must provide proof that your nominated representative(s) have the authority to remotely manage your End Users' Compatible Devices in all respects. You agree that you are responsible for any changes your nominated representative(s) make to your T-MDM platform or Compatible Devices using your login.

5.8 You are responsible for keeping your information safe by managing your own passwords and personnel who have access to your T-MDM platform. If you issue any password to your T-MDM platform to any third party, you are responsible for managing that process and their access to your T-MDM platform. We recommend you change your passwords for your T-MDM platform:

(a) with reasonable regularity; and

(b) when the circumstances require it (for example, where your nominated representative(s) change or when you suspect an unauthorised person has access to any passwords or login credentials).

5.9 To the extent permitted by law, we are not responsible for security or privacy breaches arising from or caused by the mismanagement of your passwords by you, your nominated representative(s) or your End Users. To the extent that you have failed to complied with clause 5.8, we are not responsible for the actions of unauthorised third parties who access your T-MDM platform or any information about you or your End Users using your passwords.

Using the T-MDM service

5.10 The T-MDM service will only work when Compatible Devices are turned on and connected to the internet.

5.11 The available features and functions of the T-MDM service vary depending on your Compatible Devices and the T-MDM platform you have chosen. Some of the features and functions of your T-MDM service may include allowing you to:

(a) monitor Compatible Devices;

(b) change settings on Compatible Devices;

(c) install software on Compatible Devices; and

(d) and send messages to Compatible Devices.

5.12 Not all features and functions are compatible with all Compatible Devices. Some features and functions may be enhanced over time.

5.13 Before you register a Compatible Device or use your T-MDM service to access or interact with a Compatible Device, you must obtain all necessary consents and make all necessary disclosures to each End User of that Compatible Device to enable you to lawfully use the T-MDM service (for instance, under any applicable privacy or workplace surveillance laws).

5.14 You must not, and must ensure that each of your End Users does not, use your T-MDM service to engage in conduct which is unlawful, fraudulent or negligent. You are responsible for the conduct, acts and omissions of:

(a) your nominated representative(s);

(b) each of your End Users; and

(c) or any other person when they are using your T-MDM service.

Client Access Licence Fees

5.15 If a Compatible Device you have registered on your T-MDM platform:

(a) has a mobile service which is not an Eligible Telstra Mobile Plan (see clause 5.24 for a list of the Eligible Telstra Mobile Plans); or

(b) is Wi-Fi only,

5.16 ("**CAL Devices**") then you must take a Client Access Licence ("**CAL**") for that Compatible Device and we will charge you a monthly fee for that CAL ("**CAL Fee**").

5.17 The amount of your CAL Fee depends on the number of CAL Devices you have registered on your T-MDM platform, and therefore may vary each month depending on the number of CAL Devices you have on your T-MDM platform during that month. We determine the number of CAL Devices you have on your T-MDM platform and calculate your CAL Fee on the 15th day of each calendar month.

5.18 We use the table below to calculate your CAL Fee:

	Monthly CAL Fee per CAL Device	
Number CAL Devices	**T-MDM Shared Platform** **Monthly (GST incl.)**	**T-MDM Dedicated Platform (GST incl.)**
1-300	$5.00	NA
301-1000	$5.00	$6.00
1001-2000	$4.50	$5.50
2001-3000	$4.00	$5.00
3001-4000	$3.50	$4.50
4001-5000	$3.00	$4.00

5.19 If you have chosen the T-MDM Dedicated Platform, you must have, and continue to have, at least 300 Compatible Devices registered on your T-MDM Dedicated Platform on the 15th day of each calendar month, if you have less than 300 Compatible Devices registered on your T-MDM Dedicated Platform, we may do either or both of the following, in our sole and absolute discretion:

(a) charge you a CAL Fee for the missing number of Compatible Devices to bring the total number of Compatible Devices registered on your T-MDM platform to 300; and

(b) terminate your T-MDM service by giving you 30 days' notice.

5.20 Clause 0 does not apply to the Trial Period or the three months following the Trial Period

("**Grace Period**") during which you can register 300 or more Compatible Devices on your T-MDM Dedicated Platform. Clause 0 will apply the day after the Grace Period finishes.

5.21 Your CAL Fee will be charged to your nominated billing account in arrears.

5.22 Your CAL Fee only covers a Compatible Device licence for your T-MDM platform. You must separately pay for any data usage fees and charges associated with your Compatible Devices connecting to the T-MDM platform. For the use of the T-MDM service outside of Australia, International Roaming charges apply (see Part I – Heading Overseas (International Roaming) section of Our Customer Terms for more details).

To see these terms –business and government customers click here.

Term and termination

5.23 Your T-MDM service runs on a month to month basis. You can cancel a CAL at any time by de-registering the relevant CAL Device on the T-MDM platform. Note, any CAL Device registered on the T-MDM platform on the 15th day of the month will incur a CAL Fee.

T-MDM Included With Eligible Telstra Mobile Plans

5.24 Access to your T-MDM service is available at no additional cost on a month-to-month basis for any Compatible Device that has a mobile service with any eligible Telstra mobile plan set out in the table below ("**Eligible Telstra Mobile Plans**").

Eligible Telstra Mobile Plan	T-MDM Shared Platform	T-MDM Dedicated Platform
Telstra Mobile Connect Solution ("TMCS")	Yes	Yes
Telstra Mobile Broadband plans ($100 and above minimum committed spend level per month)	Yes	Yes
Enterprise Mobile Broadband plans	Yes	Yes
Corporate Mobile Plus plans ($40 and above minimum committed spend level per month)	Yes	Yes
T-MDM Bolt-On Plan	Yes	Yes

5.25 From time to time, we may add additional mobile plans to the Eligible Telstra Mobile

Plans, at our discretion.

5.26 You must pay separately for any data usage fees and charges associated with the use of your T-MDM service and your Eligible Telstra Mobile Plan, as set out in Our Customer Terms. For use of the T-MDM service outside of Australia, International Roaming charges apply (see Part I – Heading Overseas (International Roaming) section of Our Customer Terms for more details).

To see these terms –business and government customers click here.

5.27 If you cancel your Eligible Telstra Mobile Plan and your Compatible Device is still registered on your T-MDM platform, that Compatible Device will be treated as a CAL Device and applicable CAL Fees will apply.

T-MDM Bolt-on Plan

5.28 If you are an Eligible Customer, for any Compatible Device that has a Telstra Business or Telstra Enterprise and Government post-paid mobile plan that is not an Eligible Telstra Mobile Plan, you can bolt-on access to the T-MDM service for that Compatible Device, in which case that Compatible Device will be treated as having a mobile service with an Eligible Telstra Mobile Plan.

	T-MDM Shared Platform	**T-MDM Dedicated Platform**
T-MDM Bolt-On Plan	Yes	Yes

5.29 If you choose to add the T-MDM Bolt-on Plan, then we will charge you, in advance, a monthly fee of $5 (including GST) for each Compatible Device to which you add the T-MDM Bolt-on Plan.

5.30 Your monthly fee only covers access to the T-MDM platform. You must pay separately for any data usage fees and charges associated with the use of T-MDM service and your post-paid mobile plan as set out in Our Customer Terms.

5.31 For the use of the T-MDM service outside of Australia, International Roaming charges apply (see Part I – Heading Overseas (International Roaming) section of Our Customer Terms for more details).

To see these terms –business and government customers click here

5.32 You can cancel your T-MDM Bolt-on Plan at any time on written notice to us. If you cancel your T-MDM Bolt-on Plan and your Compatible Device is still registered on your

T-MDM platform, that Compatible Device will be treated as a CAL Device and applicable CAL Fees will apply. We do not refund the fees for the unused portion of the month.

5.33 If you cancel your T-MDM Bolt-on Plan and also de-register your Compatible Device from the T-MDM platform, you will no longer be charged CAL Fees for that Compatible Device.

Advanced Content Collaboration on the T-MDM Shared Platform

5.34 When you are using the T-MDM Shared Platform, you can purchase additional content collaboration features that allow for mobile device document editing and advance document sharing ("Secure **Content Locker Collaborate**").

5.35 Secure Content **Locker** Collaborate allows End Users to share company documents with other End Users and edit those documents on their Compatible Devices.

5.36 When you or any of your End Users use Secure Content Locker Collaborate on a Compatible Device, we give you a Secure Content Locker Collaborate Client Access Licence for that Compatible Device, which allows you and your End Users to use advanced content collaboration features in your T-MDM Shared Platform ("**SCL CAL**"), and we charge you a monthly fee for that SCL CAL ("**SCL CAL Fee**").

5.37 The amount of your SCL CAL Fee depends on the number of your Compatible Devices using Secure Content Locker Collaborate, and therefore may vary each month depending on the number of Compatible Devices using the Secure Content Locker Collaborate. We determine the number of your Compatible Devices using the Secure Content Locker Collaborate and calculate your SCL CAL Fee on the 15th day of each calendar month.

5.38 We use the table below to calculate your SCL CAL Fee:

Number of Compatible Devices using the Secure Content Locker Collaborate	**Monthly SCL CAL Fee per Compatible Device using the Secure Content Locker Collaborate (incl. GST)**
1-1000	$5.00
1001-2000	$4.50
2001-3000	$4.00
3001-4000	$3.50

Number of Compatible Devices using the Secure Content Locker Collaborate	Monthly SCL CAL Fee per Compatible Device using the Secure Content Locker Collaborate (incl. GST)
4001-5000	$3.00

5.39 Your SCL CAL Fee will be charged to your nominated billing account in arrears.

5.40 You must pay separately for any data usage fees and charges associated with your use of the Secure Content Locker Collaborate with your Compatible Devices. For use of your T-MDM Shared Platform and Secure Content Locker Collaborate outside of Australia, International Roaming charges apply (see Part I – Heading Overseas (International Roaming) section of Our Customer Terms for more details).

To see these terms –business and government customers click here.

5.41 You can cancel your SCL CALs at any time by de-registering your Compatible Devices using the Secure Content Locker Collaborate on your T-MDM platform. Note, any SCL CAL device registered on the T-MDM platform on the 15th day of the month will be charged a SCL CAL Fee.

Cloud Storage with the T-MDM Shared Platform

5.42 With the T-MDM Shared Platform you will receive at no extra charge to you 25GB of cloud storage that can be used to upload company documents and materials that can be shared across all your Compatible Devices.

5.43 If you require additional cloud storage, you can take up a 12-Month Cloud Storage set out in the table below.

12-Month Cloud Storage	Price per annum, paid in advance (incl. GST)
25GB	$550.00
50GB	$1,000.00
100GB	$1,800
500GB	$8,000
1TB	$13,000

5.44 At the end of the relevant 12-month period for your 12-Month Cloud Storage, your 12-

Month Cloud will be automatically renewed and you will be charged for another 12 months in advance. If you do not want to renew your 12-Month Cloud Storage, you can notify us at any time, in which case your 12-Month Cloud Storage will be cancelled and all documents and content in your cloud storage will be deleted. It is your responsibility to make copies of any documents and content in your Cloud Storage before we delete such documents and content.

5.45 If you cancel your 12-Month Cloud Storage before the end of the relevant 12-month period for your 12-Month Cloud Storage, we will not refund you the fees you paid for your 12-Month Cloud Storage.

Professional Software Installation with T-MDM Shared Platform

5.46 The Secure Email Gateway and Mobile Access Gateway features are available to existing and new T-MDM customers. Each feature requires software to be installed at your premises and on your computer hardware, for example your computer server.

5.47 If you have chosen the T-MDM Shared Platform, we will offer you a fixed price for installing the relevant software, provided that you supply the installed pre-requisite computer hardware at your own cost. If you advise us that you would like to use the Secure Email Gateway and Mobile Access Gateway features, we will give you the technical pre-requisites and you will need to comply with these technical pre-requisites before the software can be installed.

5.48 If you comply with the technical pre-requisites then we will install the software remotely over the internet on your system.

5.49 The table below sets out the price for the remote installation of software for one server. Multiple installations will incur multiple charges.

Software	Price per installation per server (including GST)
Secure Email Gateway	$1,200 per installation per server
Mobile Access Gateway	$1,200 per installation per server

Onboarding Service for the Shared Platform and Dedicated Platform

5.50 We can assist you to setup and configure the T-MDM platform over a web conference (up to 4 hours). You must participate in this web conference.

5.51 We will perform the following activities during a web conference as part of the

Part K – Enterprise Mobility Management

Onboarding Service:

(a) upload a maximum of 10 users (e.g. email addresses, names, credentials);

(b) assists you to create and upload an Apple Push Notification Service certificate;

(c) configure system generated messages (e.g. enrolment message, enrolment terms of use, compliance messages);

(d) configure device agent settings to support GPS;

(e) enable and configure telecom management features to assist you monitor data usage;

(f) create settings for Compatible Devices (profiles);

(g) create applications groups (required and blacklisted apps);

(h) setup compliance policies for compromise status, applications, roaming and data usage; and

(i) show you how to enrol a single Compatible Device and check that all the settings are pushed correctly.

5.52 The following activities are not included in the scope for the Onboarding Service:

(a) troubleshooting device settings or applications;

(b) installation of software (e.g. Secure Email Gateway and Mobile Access Gateway);

(c) integration with your IT systems (e.g. SharePoint, Certificate Services);

(d) the ongoing management of your users, devices and settings;

(e) enrolment of devices (Telstra will enrol a single device to check that settings are pushed correctly); and

5.53 You must complete the following activities before we can provide the Onboarding Service:

(a) give us a login to the T-MDM portal so settings can be configured on your behalf; and

(b) complete and execute a document that defines all the users, settings, policies and applications you want setup. We will supply you with this document and explain the information required from you.

5.54 The table below sets out the price for the Onboarding Service.

Service	Price including GST
Onboarding Service	$700

Free 30 day trial for the Shared Platform and Dedicated Platform

5.55 When you take up a T-MDM service, you will receive a free 30 day trial. This trial ends 30 days after you receive a welcome email from Telstra with your login ("**Trial Period**"). When you first sign up for your T-MDM service, you must nominate on your application form an existing Telstra mobile account number for billing purposes.

5.56 During your Trial Period:

(a) you may register on your T-MDM platform a maximum of 25 CAL Devices, without having to pay CAL Fees for CAL Devices. However, if during the Trial Period you register more than 25 CAL Devices in your T-MDM platform, then you must pay the relevant CAL Fees for each CAL Device that you register beyond the 25th Compatible Device;

(b) if you have chosen the T-MDM Shared Platform, you may also use the Secure Content Locker Collaborate feature without having to pay SCL CAL Fees. However, if you have more than 25 Compatible Devices using Secure Content Locker Collaborate, then you must pay the relevant SCL CAL Fees for each Compatible Device, after the 25th Compatible Device, that is using Secure Content Locker Collaborate;

(c) you must separately pay for any data usage fees and charges associated with the use of your Compatible Devices.

5.57 For the use of the T-MDM service outside of Australia, International Roaming charges apply (see Part I – Heading Overseas (International Roaming) section of Our Customer Terms for more details).

To see these terms –business and government customers click here.

5.58 After the Trial Period expires, starting from the day after the end of the Trial Period:

(a) you will automatically be moved to a paid T-MDM service;

(b) you will be charged the relevant CAL Fee for each CAL Device that you have registered on your T-MDM platform; and

(c) you will be charged the applicable SCL CAL Fees for each Compatible Device using the Secure Content Locker Collaborate feature.

5.59 If you do not wish to be charged fees after your Trial Period has expired, you must de-register all CAL Devices that you have registered in the T-MDM platform and all Compatible Devices using the Secure Content Locker Collaborate before the expiry of your Trial Period.

Support

5.60 Although you may have a Compatible Device, we may not be able to provide technical support for that Compatible Device unless:

(a) the device was purchased from Telstra; and

(b) the operating software of the Compatible Device has not been modified,

(c) ("Supported Devices").

5.61 Data cards and modems are not Compatible Devices or Supported Devices.

5.62 We will provide you with reasonable email support twenty four hours a day, seven days a week. This 24/7 email support includes the following assistance:

(a) logging in and T-MDM platform access;

(b) resolving problems with features and functions of the T-MDM platform not working as designed;

(c) Supported Device connectivity to your T-MDM platform; and

(d) escalation of technical faults in relation to your T-MDM platform.

5.63 The following is excluded from this 24/7 email support:

(a) training or demonstrations;

(b) customer purchased equipment configuration;

(c) third party software configuration or troubleshooting;

(d) customer or third party settings on the devices that are not working; and

(e) registering and maintaining your Compatible Devices on your T-MDM platform.

5.64 If you use a Supported Device overseas then we may only be able to provide limited support to you.

5.65 To request technical support for a Supported Device, you must contact the Telstra helpdesk at 1800 010 253 (for high severity events) or send your support query by email to tmdm@team.telstra.com. Depending on the nature of the problem, we may require you to perform troubleshooting activities.

Additional obligations and acknowledgements

5.66 Subject to any non-excludable rights under consumer protection laws in relation to our provision of the T-MDM service, while we will use reasonable care and skill in providing T-MDM:

(a) you must test any settings or software before they are sent to your End Users' Compatible Devices over the T-MDM service;

(b) we do not warrant that the T-MDM service will meet all of your or your End Users' requirements or expectations;

(c) we do not warrant or represent that the T-MDM platform is free from errors or omissions, programming bugs or viruses or secure; and

(d) the availability of the T-MDM platform may be subject to numerous factors, including routine maintenance and factors outside our control (such as malfunction in equipment or software, Internet access difficulties, or delay or failure of transmission). Accordingly, we do not warrant or represent that the availability of the T-MDM platform will be continuous or uninterrupted, that any defects will be corrected, or that the T-MDM platform or server that makes it available are free of viruses.

5.67 You may have non-excludable rights under consumer protection laws in relation to the T-

MDM service. Subject to any non-excludable rights:

(a) we exclude all liability in tort (including negligence), contract, statute or otherwise for any loss, expenses or damage, incurred by you, your End Users or a third party in connection with the provision of the T-MDM service, including (but not limited to) any:

(i) liability for illness, personal injury or death to you, your employees, agents and contractors;

(ii) loss or damage that was not reasonably foreseeable;

(iii) loss or damage that was caused by your breach of contract or your negligence; and

(iv) loss or damage caused by events outside our reasonable control (such as a malfunction in equipment or software, Internet access difficulties or delay or failure of transmission);

(b) we exclude all other warranties, rights and remedies you would otherwise be entitled to at law; and

(c) if we breach any such non-excludable rights, and it is fair and reasonable to do so, we limit our liability to correcting any error in relation to the T-MDM platform.

5.68 You must take reasonable steps to minimise the extent of any loss or damage you may suffer as a result of the provision of the T-MDM service.

5.69 You indemnify us for any loss we suffer as a result of you, your nominated representative(s) or your End Users breaching this clause 5.

5.70 You agree that we may provide your contact details and all other necessary information to AirWatch (Australia) Pty Ltd or Citrix Systems Asia Pacific Pty Ltd for the purposes of arranging installation of your software and associated services.

T-MDM Shared Platform End User Licence Agreement (AirWatch)

5.71 You and your End Users' use of the T-MDM Shared Platform is also subject to the following provisions set out in clauses 5.72 to 5.75 below (**"End User Licence Agreement"**).

5.72 The following definitions apply to the End User Licence Agreement:

Part K – Enterprise Mobility Management

(a) "**Derivatives**" mean: (i) for copyrightable or copyrighted material, any translation, abridgment, revision or other form in which an existing work may be recast, transformed or adapted; (ii) for patentable or patented material, any improvement thereon; (iii) for material which is protected by trade secret, any new material derived from such existing trade secret material, including new material which may be protected by copyright, patent or trade secret; and (iv) results of any research, tests or analysis of a party's confidential information, or intellectual or proprietary property.

(b) "**Documentation**" means only those written user guides, specifications, and manuals supplied or made available to you by Telstra or its licensors, that set forth the specifications for the Software and/or explain, facilitate, or instruct in the use of the Software, as such may be updated by Telstra or its licensors from time to time. Documentation specifically excludes, without limitation, marketing, advertising, sales, and promotional materials and any oral or email communications regarding Software capabilities or specifications.

(c) "**Embedded Software**" means any software provided as an included part of the Software that is owned by one or more third parties and licensed to Telstra or its licensors.

(d) "**Enhancements**" means (i) any revision, amendment, or modification to the Software requested by User for which User may or may not pay an agreed-upon fee to develop and provide such revision, amendment, or modification and/or (ii) Enhancements that are generally distributed by Telstra or its licensors to users who are current on maintenance services, in its sole discretion.

(e) "**Software**" means proprietary software supplied by AirWatch (Australia) Pty Ltd ACN 151 471 788 in machine-readable, object code form only and includes T-MDM, Secure Content Locker and any software related to T-MDM, including (i) the Embedded Software, if any, (ii) any Updates made available to you pursuant to any maintenance services purchased by you, and (iii) Enhancements, if any.

(f) "**Updates**" means error corrections, patches, bug fixes, new releases, new versions, and updates of the Software that are generally made available by Telstra or its licensors, and may contain substantial new features, functions of performance, and/or extensions or improvements of capabilities, provided, however, that to the extent that Telstra or its licensors, for a fee, offers to users generally (including those users who have purchased maintenance services) any new products, such products will not be included in the definition of Updates.

5.73 Subject to applicable laws and regulations in relation to our provision of the Software to

you, you acknowledge and agree that the following restrictions exist in relation to your use of the Software:

(a) you must (and you must ensure your End Users must) use industry-standard physical, logical, and electronic security and confidentiality systems to protect the Software, using at least the same degree of care you utilise for the protection of your own software and other confidential and proprietary information;

(b) you must not share with or assign, copy, sublicense, transfer, lease, rent, sell, distribute, install, or otherwise provide to any other person (other than End Users) your licence to the Software, the Software itself, any use or application of the Software or any other rights under your agreement with us;

(c) you must (and you must ensure your End Users must) use the Software solely for your internal use with your ordinary business operations, only in accordance with all applicable laws and regulations, and in a manner consistent with your agreement with us any supplemental limitations specified or referenced in the relevant agreement, if any;

(d) you must not (and you must ensure your End Users must not) use the Software except as specified or referenced in the Documentation or use the Documentation except for supporting your authorised use of the Software;

(e) you must (and you must ensure your End Users must) not modify, adapt, translate, duplicate (except as expressly allowed in your agreement with us), disassemble, decompile, reverse assemble, reverse compile, or reverse engineer, or take similar action with respect to the Software for any purpose, or otherwise attempt to discover the underlying source code of the Software, for any purpose (unless enforcement is prohibited by applicable law and then, to only the extent specifically permitted by applicable law, and only upon providing Telstra with reasonable advance written notice and opportunity to respond);

(f) for the purpose of designing, modifying, or developing software or services similar in purpose, scope, or function to the Software, you must not (and you must ensure your End Users must not) engage in competitive analysis, benchmarking, use, evaluation or viewing of the Software or Documentation or create any Derivatives based upon the Software, whether for your internal use or for license or for resale;

(g) you must not (and you must ensure your End Users must not) use the Software, and must ensure that the Software is not used, in or in conjunction with any applications where product failure could lead to injury to persons, loss of life or

severe property or environmental damage;

(h) if you use the Software to manage Compatible Devices running on the operating system known as "iOS" from Apple, you must not (and you must ensure your End Users must not) use the Software without first obtaining your own APNs Certificate from Apple; and

(i) you must not permit any person (including an End User), whether acting directly or on your behalf, to breach or violate any of the restrictions set forth in this section.

5.74 You acknowledge and agree that Telstra's licensor retains all ownership and intellectual property rights to the Software at all times. Title to the Software does not pass to you, the End User, or any third party. Telstra and its licensors disclaim, to the extent permitted by applicable law, its liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Software. Telstra and its licensors will not be required to perform any obligations, nor will Telstra or its licensors incur any liability, except as previously agreed between them in writing.

5.75 You acknowledge and agree that the Software is subject to United States of America export control laws and regulations and may be subject to export or import regulations in other countries. These laws and regulations include licensing requirements and restrictions on destinations, end users, and end use. You agree to comply with all United States of America domestic and international export and import laws and regulations that apply to the Software and acknowledge that you have the responsibility to obtain any and all necessary licenses to export, re-export, or import the Software. More specifically, you covenant that you will not, directly or indirectly, sell, export, re-export, transfer, divert, or otherwise dispose of any the Software, source code, or technology (including products derived from or based on such technology) received from Telstra under your agreement with Telstra, to any other person, entity, or destination prohibited by the laws or regulations of the United States of America, without obtaining prior authorisation from the competent government authorities as required by those laws and regulations.

T-MDM Dedicated Platform – Supplier End User Terms (Citrix)

5.76 In this Supplier End User Terms section:

(a) "you" or "your" means the customer;

(b) "we", "us" or "our" means Telstra; and

(c) T-MDM service means the XenMobile Service.

5.77 You:

(a) must not resell or resupply the T-MDM service without our prior written consent;

(b) must use the T-MDM service in accordance with applicable laws;

(c) must provide us (and our subcontractors) with all information we request in connection with the T-MDM service, including but not limited to:

(i) the address of your registered office and other office locations;

(ii) the locations from which you will use the T-MDM service; and

(iii) the locations at which you will install software we provide to you as part of the T-MDM service;

(d) must not change the location, or install at another location, software we provide to you as part of the T-MDM service unless we agree otherwise with you;

(e) must comply with our reasonable directions in relation to your use of the T-MDM service;

(f) must comply with all our directions in relation to your use of software we provide you with as part of the T-MDM service;

(g) agree that we may suspend our supply of the T-MDM service where that supply is, or is likely to be, contrary to law (including any export control laws);

(h) except where permitted by law, must not modify or reverse engineer the object code of the any software we provide you as part of the T-MDM service without our prior written consent;

(i) must not use the T-MDM service in a way that interferes (or threatens to interfere) with the efficiency and security of the T-MDM service or another person's services;

(j) must not use the T-MDM service to distribute any form of malicious, destructive or harmful code (including without limitation Trojan horses and worms) or any instructions activating such code;

(k) must not use the T-MDM service to menace, harass or stalk any person whether intentionally or unintentionally;

(l) must not use the T-MDM service to distribute material that is defamatory, obscene or could cause offence or harm; and

(m) must not use the T-MDM service in a manner that infringes any other person's intellectual property rights, confidential information or other rights.

5.78 You agree that you must ensure that your End Users comply with the terms of paragraphs 5.77(a) to (m) above. We may suspend or cancel the T-MDM service if you do not comply with, or we believe on reasonable grounds that you do not comply with, the terms of paragraphs 5.77(a) to (m) above.

5.79 You agree that personal information will be collected by us as part of our provision of the T-MDM service to you and:

(a) we may use that personal information for the purpose of delivering the T-MDM service to you;

(b) we may provide your personal information to our subcontractors in order to deliver the T-MDM service to you and those subcontractors may transfer that personal information to their subcontractors and corporate group members in order to provide the T-MDM service to you;

(c) we may use that personal information communicate with you or ask our subcontractor to communicate with you in relation to the T-MDM service;

(d) we, and our subcontractors, may use that personal information to ensure that we, and our subcontractors, comply with applicable laws (including export control laws);

(e) we, and our subcontractors, may use that personal information for research and analysis aimed at improving our products and services as well as the products and services of our subcontractors, however, we will de-personalise any personal information used and aggregate it for use in this research and analysis; and

(f) we may transfer that personal information, and that personal information may also be accessed from, outside Australia including to, and from, countries including India, Ireland, Pakistan, the United Kingdom and the United States of America.

PART B – Terms and conditions for your specific parts of your T-MDM service

Zimperium Intrusion Protection Solution

5.80 What is Zimperium Intrusion Protection Solution?

5.81 The Zimperium Intrusion Protection Solution (**zIPS App**) is an app built with a cyber-attack detection engine that monitors both corporate-owned and BYO mobile devices for malicious behaviour, protecting against threats on the device and on Wi-Fi and cellular networks.

Eligibility

5.82 The zIPS App is only available through and can only operate with your T-MDM service.

5.83 To be able to use the zIPS App:

(a) your End Users must have a compatible device with an Android v5+ or iOS v8+ operating system with sufficient access to the internet. We can provide you with details of compatible browsers and devices on request; and

(b) the zIPS App must be downloaded or installed on the device of each of the relevant End Users.

5.84 You can install on the relevant devices the zIPS App by:

(a) ensuring that your End Users download the zIPS App from the T-MDM enterprise app catalogue; or

(b) pushing the zIPS App to the relevant devices as part of your company policy through your T-MDM service.

Charges

5.85 There is no additional charge for your zIPS App, however:

(a) mobile data is required to download the zIPS App and the zIPS App itself uses mobile data when checking security threats. Standard mobile data may rates apply; and

(b) if we develop and incorporate additional security features and functions into the zIPS App, we may charge you for these additional features and functions. We will provide notice of any such feature and function changes, and you will be given the

choice to opt in or out of using (and, where applicable, paying for) those new features and functions.

Additional terms

5.86 You acknowledge that we rely on a third party service provider to supply the zIPS App service to you and your End Users. You must comply, and ensure that your End Users comply, with the terms set out in sections 5.87 to 5.99 below (**Zimperium Terms**), which we are required to impose on you by our third party service provider.

5.87 Rights to use the zIPS App: You may only install one copy of the zIPS App on each device. You

5.88 Restrictions on the use of your zIPS App: You and your End Users:

(a) must not use the zIPS App for any purpose other than for your own personal or internal business use;

(b) must only use the zIPS App in accordance with any applicable documentation we or our third party service provider provide to you, and only for the purpose of evaluating, managing, and protecting the security of mobile devices and wireless networks that you own or control;

(c) must not use the zIPS App to attack, probe, assess the security of, or interfere with any third party's network, device or other target without that third party's express, informed authorization;

(d) must not disclose any vulnerability discovered, reproduced, or confirmed through the use of the zIPS App except in accordance with industry accepted vulnerability disclosure practices;

(e) must not:

(i) copy, modify or distribute the zIPS App for any purpose;

(ii) transfer, sublicense, lease, lend, rent or otherwise distribute the zIPS App to any third party;

(iii) decompile, reverse-engineer, disassemble, or create derivative works of the zIPS App;

(iv) make the functionality of zIPS App available to multiple users through

any means, other than as permitted under this section of Our Customer Terms;

(v) use the zIPS App in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with this section of Our Customer Terms or any applicable documentation provided to you by us or our third party service provider;

(vi) access or use any areas of the zIPS App for which we have not granted you authorization, or tamper or interfere with our computer systems or technical delivery systems (or that of our third party service providers);

(vii) use the zIPS App to transmit any unsolicited advertising, junk mail, spam or other form of solicitation; or

(viii) encourage or enable anyone to commit any act or omission set out in this section 5.88(e);

5.89 Indemnity and enforcement: You indemnify us and our third party service providers (including our representatives and the representatives of our third party service providers) fully against any claims, liabilities, costs, expenses, and other harm arising from your unauthorized use of the zIPS App or any other breach of these Zimperium Terms. We and/or our third party service provider may, but have no obligation to, monitor compliance with the prohibitions set out in section 5.88, and we and/or our third party service provider may investigate and prosecute any breach of section 5.88 and/or involve and cooperate with law enforcement authorities in prosecuting users who violate these Zimperium Terms.

5.90 Acknowledgements: You acknowledge and agree that improper use of the zIPS App could significantly harm your network and/or devices, and subject to the terms of Our Customer Terms, you assume all risks associated with your use.

5.91 Intellectual property: All copyrights, patents, trademarks, and other intellectual property rights in the zIPS App remain our property or that of our licensors at all times. You and your End Users may not remove, alter, or obscure any copyright, trademark, or other proprietary rights notices appearing on the zIPS App. If you provide us or our third party provider with any suggestions, comments, or other feedback regarding the zIPS App (**Feedback**) you acknowledge and agree that such Feedback will become our exclusive property or that of our third party service provider, and we or our third party service provider may use (or not use) any such Feedback in any manner and for any purpose, without compensation to you and without implying or creating any interest on your part in any of our or our third party service provider's products or services that may be based on such Feedback. You irrevocably assign, and must ensure that your End Users irrevocably assign, to us or our third party service provider all right, title, and interest in any Feedback

you provider.

5.92 Changes to the zIPS App: The zIPS App may change from time to time (for example, we may push updates to your devices, increase or decrease server capacity, or modify the user interface). We will notify you of detrimental changes to your zIPS App where required by, and in accordance with, the General Terms of our Customer Terms.

5.93 Data collection and transmission:

(a) In order for the zIPS App to identify patterns associated with security attacks and to perform other functions for which it is designed, it will gather and transmit to us and our third party service provider certain technical information, user data, and metadata associated with your End Users' devices and use of the zIPS App, including device IDs, MAC addresses, user names and email addresses, IP configurations, stored sessions, open ports, captured credentials, network metadata, and device operating system, status, version, and configuration (collectively, "**Data**").

(b) You acknowledge, consent and agree, and must ensure that your End Users acknowledge, consent and agree, to the collection, transmission, storage, monitoring, copying, processing, analysis and use of the Data by us and our third party service provider to administer and provide you the zIPS App, to develop and improve the zIPS App and other products and services, and to monitor compliance with these Zimperium Terms.

(c) You acknowledge and agree, and must ensure that your End Users acknowledge and agree, that we or our third party provider may transmit your Data to or from locations in the United States, Europe, and other countries or jurisdictions outside of Australia.

(d) We or our third party provider may also disclose Data as needed to cooperate with law enforcement activities and otherwise to fulfil any legal obligations and protect our legal rights or that of our third party service provider.

(e) You are solely responsible for securing any privacy-related rights, and permissions from your End Users in relation to the zIPS App, consistent with this section 5.93, as may be required by Australian law (or any other local law, as applicable) or by your organisation's internal policies.

5.94 Third-party software:

(a) The zIPS App may be accompanied by or utilise certain third-party software

components, libraries or applications that are distributed (with or without modifications) under open-source licensing terms (**Open-Source Components**).

(b) Your rights, and the rights of your end users, with respect to the Open-Source Components are, to the extent of any conflict with these Zimperium Terms, governed by and subject to the terms of the open-source licenses under which they are distributed. You are responsible for complying, and ensuring that your End Users comply, with those licenses. Please refer to our website for more specific information regarding the Open-Source Components that we redistribute and the licenses that apply to them. You may not assume or infer that we or our third party provider endorse, or that we have reviewed, verified, or authenticated, any Open-Source Components or other third-party software that may be furnished with, available through, or used in connection with the zIPS App.

(c) Open-Source Components and any other third-party software, and the information or results provided by them, may be unreliable, inaccurate, incomplete, delayed, or otherwise defective. To the extent permitted by law, we and our third party provider make no representations, warranties, or guarantees in connection with any third-party software or the information or results provided by it. To the extent permitted by law, you acknowledge sole responsibility for and assume all risk arising from your use of or reliance on any third-party software.

5.95 Verification and Audit:

(a) We or our third party provider may (but are not required to) monitor the use of the zIPS App, including by tracking the relevant device IDs and license keys associated with the device on which the zIPS App is used, for purposes of verifying compliance with these Zimperium Terms. In addition, you agree to track and keep records of the End Users and devices using the zIPS App and promptly notify us and our third party service provider if you learn of any unlicensed or unauthorised use. At our written request or at the written request of our third party service provider, you will provide us or our third party service provider (as applicable) with a certification signed by you (or, if you are an organization, by an officer of the organization) verifying that the zIPS App is being used in compliance with these Zimperium Terms.

(b) We or our third party service provider may, at any time while you are using the zIPS App or for one year thereafter, upon reasonable written notice, audit your use of the zIPS App. We and our third party service provider may use a third-party organisation to assist us in conducting such an audit. You agree to cooperate, and must ensure that your End Users cooperate, with us or our third party service provider in such audit and will promptly make available to us or our

third party service provider all information, equipment and materials that we or our third party service provider reasonably require to conduct such an audit.

5.96 Termination

(a) Any rights for us to suspend your use of and access to the zIPS App are in addition to our rights to suspend your T-MDM service.

(b) We may suspend your use of and access to the zIPS App as we deem appropriate to prevent, investigate, or otherwise address any suspected misuse of the zIPS App.

(c) Upon expiration or termination of your T-MDM service or of your right to use and access the zIPS App, you must to promptly and permanently delete, and must ensure that your End Users promptly and permanently delete, all copies of the zIPS App that are on your End Users' devices or otherwise in your possession or control. The provisions of sections 5.88, 5.89, 5.90, 5.91, 5.95, 5.97, 5.98 and 5.99, will survive any and continue to apply after expiration or termination of your T-MDM service or your right to use and access the zIPS App, solely with regards to your and your End Users' use of the zIPS App.

5.97 Limitation of Liability: To the maximum extent permitted by law and subject to section 5.99:

(a) our total liability, and the total liability of our third party service provider, to you from all causes of action and under all theories of liability in connection with the zIPS App will not exceed US$50;

(b) we and our third party service provider will not be liable to you for any indirect, incidental, special, consequential or punitive damages, or for costs of substitute goods or services, or for loss of profits, data, use, goodwill, or other intangible losses, arising in any way out of these terms or resulting from your access to, use of, or inability to access or use the software and/or cloud application, whether based on warranty, contract, tort (including negligence) or any other legal theory, whether or not we have been informed of the possibility of such damage, and even if a remedy set forth herein is found to have failed of its essential purpose; and

(c) you acknowledge and agree that it is your responsibility to implement back-up plans and other safeguards appropriate for the value of the networks, devices, data, and systems with which you use the zIPS App and, accordingly, that the exclusions and limitations of damages and liability in this section 5.97 and in

section 5.98 are reasonable.

5.98 Disclaimers: Subject to section 5.99:

(a) you understand and agree that the zIPS App is provided to you "as is" and on an "as available" basis;

(b) to the fullest extent permissible under applicable law, we and our third party provider disclaim any and all warranties, whether express, implied, statutory or otherwise, including any implied warranties of merchantability, fitness for a particular purpose, quiet enjoyment or non-infringement, and any warranties arising out of course of dealing or usage of trade; and

(c) we and our third party service provider make no warranty that the zIPS App will meet your requirements, will detect or prevent all security threats or vulnerabilities, or be available on an uninterrupted, secure, or error-free basis, or that any patch applied for a detected security threat will be effective.

5.99 Your consumer rights:

(a) Our goods and services come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

(b) If the *Competition and Consumer Act 2010* (Cth) or any other legislation states that there is a guarantee in relation to the zIPS App, and our liability for failing to comply with that guarantee cannot be excluded but may be limited, sections 5.97 and 5.98 do not apply to that liability and instead our liability for such failure is limited (at our election) to, in the case of a supply of goods, our replacing the goods or supplying equivalent goods or repairing the goods, or in the case of a supply of services, our supplying the services again or paying the cost of having the services supplied again.

6 Mobile Workspace

What is Mobile Workspace?

6.1 Mobile Workspace is an end-to-end service for approved laptops, 2-in-1s or convertibles devices ("**Devices**") designed to be used as mobile workspace by your employees or

contractors whom you authorise to use a Device ("**End Users**"), and more specifically, comprises the following:

(a) coordination of the provisioning and on-site delivery of Devices;

(b) Device staging and configuration;

(c) end-to-end managed services, including consulting, design and implementation, threat detection management, service desk and End User support services, Device management platforms and business intelligence capabilities;

(d) data connectivity for your Devices; and

(e) Device lifecycle management,

("**Mobile Workspace**").

6.2 You acknowledge and agree that:

(a) the Devices, as well as the provisioning and delivery of the Devices, are provided by the Lease Provider under the agreement between you and that third party Lease Provider contemplated in clause 6.3(d) below; and

(b) the product warranty in relation each Device is provided to you by the Lease Provider or the relevant Device manufacturer (as applicable).

Eligibility, requirements and limitations

6.3 To be able to receive the Mobile Workspace service from us, you must:

(a) have a valid ACN, ABN or ARBN;

(b) not have any other mobile offering on the Telstra account under which you acquire the Mobile Workspace service;

(c) enter into a separate agreement with us for the supply of Mobile Workspace;

(d) enter into a Device leasing arrangement with Brightstar Logistics Pty Limited, or any other third party we notify you from time to time ("**Lease Provider**"). While you will need to enter into a Device leasing agreement with a third party, you will order your leased Devices through us;

(e) order initial planning, implementation and transition (if applicable) services from

us in relation to your Mobile Workspace solution ("**Implementation Services**"). Those Implementation Services will be agreed in a Statement of Work and provided on the terms set out in the Professional Services section of Our Customer Terms.

6.4 Mobile Workspace is:

(a) not available to Telstra Wholesale customers or for resale. You must not re-supply Mobile Workspace services to any third party;

(b) only available in relation to Devices that are being leased to you as contemplated in clause 6.3(d); and

(c) only compatible with the VMWare Workspace One Advanced mobile device management ("**MDM**") platform provided as part of the Mobile Workspace service ("**MDM Platform**").

Implementation

6.5 As part of the Implementation Services, we will work with you to create and agree upon a Customer Services Engagement Manual ("**CSEM**"), documenting the roles, responsibilities, and agreed processes that we will follow to deliver your Mobile Workspace service.

6.6 The CSEM is the single point of reference for both you and us on the operational aspects of your Mobile Workspace service. Changes to the CSEM require mutual agreement between you and us. You may request changes at any time through the change management process documented in the CSEM. Changes to the CSEM may incur additional cost.

6.7 We may, but are not required to, act on instructions of your authorised administrators (other than changes to authentication processes) that are inconsistent with the processes documented and agreed in the CSEM.

End Users and Registered Devices

6.8 We will only provide Mobile Workspace in respect of your End Users we have authenticated in accordance with the processes agreed in the CSEM, who have enrolled their Device on the MDM platform ("**Registered Devices**"), and that Device is turned on and connected to the internet.

Part K – Enterprise Mobility Management

Included features

6.9 We will provide to you the following as part of your Mobile Workspace service:

Service Feature	Description
End-to-end management of your MDM Platform	We will setup and configure your MDM Platform, as a Telstra dedicated environment used for shared multiple / multi-tenant customers. We will maintain your MDM Platform on an ongoing basis, including deploying updates in a timely manner, and implementing your policies agreed in the CSEM on and through the MDM Platform to your End Users' Registered Devices. Your MDM Platform (supporting mobile device management) will be integrated into your supported enterprise mobility management ("**EMM**") platform, (supporting mobile content and mobile application management) ("**EMM Platform**"). As part of the end-to-end management of your EMM and MDM Platforms we will: • Deploy; o VPN profiles including for certificate based authentication, security and privacy, disk encryption, firewall, and anti-virus software; o up to 5 public apps to Registered Devices; o WiFi restrictions, VPN, email, web clip and policy / security server configurations to Registered Devices; o install and record instance and approved licenses to Registered Devices; • Assist with; o enrolment and enrolment end user support; o lost and stolen device end user support; o MDM agent app and device configuration end user support; o email reverse proxy support; o anti-virus and device firewall support; • Manage; o maintenance of MDM and EMM Platforms, including deployment of timely updates; o updates to enrolment documents;

Part K – Enterprise Mobility Management

Service Feature	Description
	o maintenance of use or device certificates; o profile and policy changes; o administrator role management; o compliance rules and enforcement actions; o change management assistance; • Control; o self-service reporting access and EMM portal training.
End User Support	We will provide a help desk available by phone, email and an online portal, and will support your End Users. Unless agreed otherwise in your separate agreement with us: • the help desk is available 24x7 for the following requests: o reporting and remediation of severity 1 incidents; o End User support for lost or stolen Devices (e.g. locking Devices, removing corporate data and access, locating Devices or resetting to factory settings); o password reset / unlocking device; and o incident support for End Users travelling overseas; and • for all other requests and issues, the help desk is available Monday to Friday 8am to 8pm AEDT, excluding public holidays (in Sydney, Australia).
Business Reporting Insights	We will provide your nominated admin user with access to pre-configured core reports through an online portal, with information about how your business consumes the managed service, service desk utilisation on incidents & requests, change management, licence, mobile threat, operating system and fleet reports.
VMWare Workspace ONE Advanced (or, the MDM Platform)	Mobile Workspace includes VMWare Workspace ONE Advanced licences for each of your Registered Devices. As part of Mobile Workspace, we will provide a dedicated instance of the MDM Platform, as a Telstra dedicated environment used for shared multiple / multi-tenant customers.

Service Feature	Description
Fleet and Device Lifecycle Management	We will also provide assistance with: • Device leasing and logistics; • Device staging, provisioning (including SIM card installation), configuration, allocation and deployment; • management of Device repairs and replacements; • monthly reporting on Devices ordered, deployed, repaired, asset allocation and Device hardware details (being details of the Device's make, model and operating system); and • end-of-life services (including removing corporate access, wiping and disposing of end-of-life Devices).
Connectivity (Mobile Workspace Data Plan)	Your Mobile Workspace will include a 36-month data plan, which will provide you with a monthly data allowance for each Device and which is shared across all your Registered Devices ("**Mobile Workspace Data Plan**").

Optional Features

6.10 You may choose to improve Mobile Workspace experience with one or more of the following optional services:

Optional Service Feature	Description
24x7 End User Support	If you take up optional 24x7 End User Support, we will provide extended 24x7 help desk availability for all incidents and requests, excluding the following: (a) change approval activities; (b) change management; (c) fleet services that rely on logistics; and (d) any third-party provided service including the MDM or EMM Platforms) that is available only during business hours.

Mobility Service Manager	If you take up optional Mobility Service Manager service, we will provide a service manager who will enhance your Mobile Workspace managed service with proactive consulting and collaboration in relation to: (a) your solution; (b) mobile OS updates; (c) service reporting; (d) planning; and (e) enhancements. The scope of the Mobility Service Manager service will be agreed in a Statement of Work and provided on the terms set out in the Professional Services section of Our Customer Terms.
Professional Services	Any further or additional professional services agreed in a Statement of Work on the terms set out in the Professional Services section of Our Customer Terms.
Additional Accessories	You may order additional Accessories to use with your Devices. The details of those Accessories will be agreed in your separate agreement with us.

Mobile Workspace Data Plan

Your Mobile Workspace Data Plan

6.11 The monthly data allowance for your Mobile Workspace Data Plan will be set out in your separate agreement with us ("**Monthly Data Allowance**").

6.12 For each Registered Device in relation to which you order a Mobile Workspace service, you will receive a Monthly Data Allowance for that Registered Device. The Monthly Data Allowances for all your Registered Devices are pooled and shared across all your Registered Devices.

6.13 Any portion of your Monthly Data Allowances not used in the relevant month does not carry over to the next month and will automatically expire at the end of that month.

International Roaming

6.14 Unless otherwise agreed in your separate agreement with us or notified by you to us:

(a) International Roaming is automatically activated with your Mobile Workspace Data Plan; and

(b) the terms of Part I – Heading Overseas – International Roaming of the Telstra

Mobile Section of Our Customer Terms apply to your use (and your End Users' use) of the International Roaming services.

6.15 If you have requested for International Roaming not to be automatically activated, your Devices will not be able to use mobile data outside of Australia, and you (or your End User) will need to contact us to activate International Roaming.

6.16 If International Roaming is activated and you (or your End Users) use a Device outside of Australia, you will receive an International Roaming Day Pass in relation to that Device. The charges and terms and conditions that apply in relation to that International Roaming Day Pass are set out in your separate agreement with us.

Data usage

6.17 When calculating data volumes:

(a) where the volume of data transferred is not a whole number of kilobytes, it is rounded up to the next kilobyte at the end of each session;

(b) 1024 bytes = 1 kilobyte (KB);

(c) 1024 kilobytes = 1 megabyte (MB); and

(d) 1024 MB = 1 Gigabyte (GB).

6.18 If you (or your End Users) exceed your Monthly Data Allowance in Australia in any given month, you will be charged 0.8 cents per MB or part thereof.

6.19 Additional charges for additional data usage capped at $500 per Mobile Workspace Data Plan, after which the network connectivity for that plan will be suspended until the end of the then-current month.

Restrictions on use

6.20 Your Mobile Workspace service and Registered Devices can only be used with your Mobile Workspace Data Plan, and your Mobile Workspace Data Plan can only be used with your Mobile Workspace service.

6.21 You understand and agree that that the *Telstra FairPlay Policy – Business Use* (as set out in Part A - General of the Telstra Mobile section of Our Customer Terms) applies to your Mobile Workspace Data Plan. Additionally, you must not use or allow others to use any service or Device connected to a Mobile Workspace Data Plan:

(a) in connection with any machine-to-machine applications (i.e. any automated telemetry, telematics or telemetrics application which links two or more systems or devices with a mobile data connection);

(b) to establish any point to point connections with another modem; or

(c) to send messages to any numbers that we reasonably believe have been set up to enable you or another person to commercially exploit our services.

Your responsibilities

6.22 You must:

(a) nominate a person to be single point of contact with Telstra for all matters in relation to your Mobile Workspace service;

(b) not make any unauthorised changes to any infrastructure, software (including email systems) or configurations that support the Mobile Workspace service without complying with clauses (c) and (d) below;

(c) notify us of any planned changes to your operating system or back-up, anti-virus or security systems:

(i) for regular changes, at least 14 days before the change is implemented, and

(ii) for emergency changes, at least 8 business hours before the change is implemented;

(d) without limiting clause 6.22(c) above, promptly notify us of any changes to your technology environment that may impact the service, including any changes to email infrastructure and network (such as firewalls and gateways);

(e) provide us with all reasonable assistance and access to your information, premises, systems and equipment (including your Devices) as requested from time to time for the purposes of providing the Mobile Workspace service to you and

your End Users; and

(f) comply with all our reasonable instructions and procedures in relation to your Mobile Workspace service.

Third Party Suppliers

6.23 Some aspects of your Mobile Workspace service may be the responsibility of a third party or conditional upon action by a third party. To the extent the CSEM defines an action as a third party responsibility:

(a) we are not responsible for any delay or inaction by the third party; and

(b) as between you and us, each responsibility of the third party is deemed to be your responsibility.

6.24 To avoid doubt, third party suppliers in clause 6.23 do not include Telstra's related entities such as BTS Mobility, or licensors of Telstra providing MDM capabilities.

6.25 You appoint us as your agent to act on your behalf in relation to any third party supplier to the extent specified in the CSEM, including entering purchase agreements on your behalf.

6.26 You authorise us to provide your contact details and all other necessary information (including confidential information) to any third party suppliers, and to instruct third party suppliers on your behalf, to the extent necessary for us to provide Mobile Workspace. Upon request, you must provide all assistance we reasonably require to provide Mobile Workspace, including authorisations to third party suppliers.

Limitations

6.27 You acknowledge and agree that:

(a) from time-to-time, we may need to implement planned outages to your MDM Platform for maintenance and upgrade purposes. We will provide you with prior reasonable notice before commencing any transfer or planned outages and will aim to cause as little impact as possible to your Mobile Workspace service when we do;

(b) we may require you or your End Users to agree to a further end user licence agreement ("**EULA**") with us (or our third party supplier) to access and use the MDM Platform, and if you or any End User refuses to enter into that EULA, we may not be able to supply and you (or that End User) may not be able to receive

and use the Mobile Workspace service; and

(c) we do not represent and cannot guarantee that Mobile Workspace (including MDM Platform) is capable of integrating with any third party software or service, unless expressly set out in your agreement with us.

Service Levels

6.28 Unless otherwise agreed in your separate agreement with us, we will use reasonable commercial efforts to meet the target response, communication frequency and resolution time set out below:

Incident Severity	Target Response Times	Target Communication Frequency	Target Restoration Times	Service Level Target
Severity 1 (Critical)	15 min	1 hours	4 hours	90%
Severity 2 (Major)	30 min	2 hours	8 hours	90%
Severity 3 (Minor)	1 hour	8 hours	1 business day	90%
Urgent Request	2 hours	12 Hours	3 business days	90%
Standard Request	3 hours	24 Hours	5 business days	90%

Severity 1 (Critical) means failure of the system with a major business impact affecting more than one End User, business critical system or process with no workaround.

Severity 2 (Major) means one or more End Users are affected by the failure of a business critical system which may have a workaround that cannot be sustained over a reasonable period of time (more than 1 day).

Severity 3 (Minor) means one End User is affected and not business critical which may have a workaround that can be sustained over a reasonable period of time (more than 1 day).

Urgent Request means a service request for one or more End Users, which has some urgency owing to business requirements or targets.

Standard Request means a service request for one or more End Users, which has no

immediate impact and the request is not business critical.

6.29 The service level targets in clause 6.28:

(a) operate during the help desk availability times, which depend on whether you have standard End User Support or the 24/7 End User Support Optional Feature; and

(b) do not apply in relation to any period of scheduled maintenance; and

(c) are targets only, you acknowledge and agree that, unless otherwise agreed in your separate agreement with us, we are not liable to you for any failure to meet the service level targets set out in clause6.28.

6.30 We will not be responsible for a failure to meet a service target to the extent that such failure is caused by your delay in actioning items that are your responsibility, a third party responsibility (as agreed in the CSEM), or that are caused by your breach of this agreement.

Charges

6.31 The charges and payment terms for your Mobile Workspace service (including any Accessory, Optional Features and Professional Services) are set out in your separate agreement with us.

Minimum Commitment and Early Termination Charges

6.32 Your Mobile Workspace service has a minimum term of 36 months ("**Minimum Term**").

6.33 If your Mobile Workspace service is terminated before the end of the Minimum Term for any reason other than for our breach:

(a) depending on the terms of your agreement with the Lease Provider, the lease for your Devices may continue, in which case you will be required to continue to pay the applicable fees in relation to the lease; or

(b) depending on the terms of your separate agreement with us, if you have purchased any Accessories from us, we may require you to pay our accessory repayments; and

(c) we may require you to pay an early termination charge equal to 25% of the monthly service charges for your Mobile Workspace service (including any Optional Features and Mobile Workspace Data Plans) multiplied by the number

of months remaining until the end of your Minimum Term.

Optional Accessories

Application

6.34 Clause 6.34 to 6.44 only applies to your purchase and our supply to you of Accessories (if any) in connection with your Mobile Workspace service, and as agreed in your separate agreement with us.

How we deliver the Accessories

6.35 We will deliver the Accessories during Business Hours to the address set out in your separate agreement with us or otherwise agreed in writing between you and us from time to time.

6.36 We will use reasonable efforts to both deliver the Accessories to you by the date we tell you and update you of delivery delays (if any). However, the supply of the Accessories depends on availability from the relevant Supplier, and so we cannot guarantee to meet any particular delivery date.

6.37 You may request special delivery for any Accessory and we'll use reasonable efforts to accommodate your request. Additional costs may apply and we will agree these costs with you beforehand.

Transfer of title and risk

6.38 Risk in any Accessory passes to you when we deliver the Accessory to you.

6.39 Title to any Accessory:

(a) remains with us until you have paid us in full for that Accessory;

(b) passes to you once you have paid the relevant fees or charges for that Accessory in full.

Repayment Plan

6.40 If your separate agreement with us indicates that you are acquiring any Accessories on a Repayment Plan, we will charge you during the applicable Repayment Term a monthly amount for that Accessory as set out in your separate agreement with us. Not all Accessories are available on a Repayment Plan.

6.41 The relevant monthly instalments for the Accessories will be reflected in your bill each month as a separate line item. If you fail to pay two or more instalments under your Repayment Plan in relation to any Accessory, we may suspend or cancel your Mobile Workspace service in whole or in part.

6.42 You can cancel your Repayment Plan at any time before the expiry of your Repayment Term for any Accessory, provided you:

(a) complete a cancellation form for cancellation of your Repayment Plan (a copy of this form can be obtained from us); and

(b) pay the outstanding balance of the applicable upfront fees for the relevant Accessory associated with that Repayment Plan.

6.43 If you cancel your Mobile Workspace service associated with any Accessory purchased under a Repayment Plan before expiry of the Repayment Term for that Repayment Plan, that Repayment Plan will be automatically terminated and you must pay the outstanding balance of the applicable upfront fees for the Accessory associated with that Repayment Plan.

Early termination

6.44 If your Mobile Workspace service or your separate agreement with us is terminated early because of your breach, you must promptly pay us for any Accessory which has been ordered or delivered before the date of termination.

Definitions

6.45 In this clause 6:

Accessories means accessories for your Devices, as set out in your separate agreement with us.

CSEM has the meaning given to it in clause 6.5.

Device has the meaning given to it in clause 6.1.

End User has the meaning given to it in clause 6.1.

Implementation Services has the meaning given to it in clause 6.3(e).

International Roaming has the meaning given to it in Part I – Heading Overseas –

Part K – Enterprise Mobility Management

International Roaming of the Telstra Mobile Section of Our Customer Terms.

Lease Provider has the meaning given to it in clause 6.3(d).

MDM has the meaning given to it in clause 6.4(c).

MDM Platform has the meaning given to it in clause 6.4(c).

Minimum Term has the meaning given to it in clause 6.32.

Mobile Workspace has the meaning given to it in clause 6.1.

Mobile Workspace Data Plan has the meaning given to it in clause 6.9.

Monthly Data Allowance has the meaning given to it in clause 6.11.

Optional Features means the optional services or features contemplated in clause 6.10.

Registered Device has the meaning given to it in clause 6.8.

Repayment Plan means a repayment plan under which you pay off the upfront charges or fees for the relevant Accessory through monthly instalments during a Repayment Term.

Repayment Term means the term for a Repayment Plan as set out in your separate agreement with us.

Supplier means the third party supplier(s) or manufacturer(s) of the various Accessories.