MOBI

Service Attachment 6

Enterprise Mobility Management (EMM)

This Service Attachment (the 'Service Attachment'), is between MOBI Wireless Management, LLC ('MOBI') ('Service Provider') having an office at 6100 West 96th Street, Suite 150, Indianapolis, IN 46278, and the Department of Administrative Services ('the State'), having its principal place of business at 30 East Broad Street, 40th Floor, Columbus, Ohio 43215 (jointly referred hereto as the 'Parties'), and it is effective as of the date signed by the State. It amends that Certain Master Service Agreement (MSA) between the Parties dated February 3, 2012.

1. Definitions

MDM – Mobile Device Management

BYOD – Bring Your Own Device

User – Subscribing Entity.

2. Description of Services

EMM platform management requires a complete perspective on all moving parts of the EMM platform and each integrated piece of the organization's technology stack. In order to build and manage nimble EMM platforms Mobi engineers design management around the following areas:

EMM Security Management

Security Management	Working with the organizations security policies…
Device Level	Organization's security policies extend to the device being deployed. Through MDM platform management, complex passcode enforcement, and device encryption, Mobi builds and maintains security policies in alignment with organizational governance.
Data Exchange Level	Through experienced containerization design, Mobi engineers secure organizational data, and equip mobile program design whether BYOD, COPE, or Corporate owned.
Policy Design Level	Global MDM platforms must be built to provide exactly what is needed to a diverse workforce or clientele. The critical center of value is in device policy design. In order to meet the mountain or variables, Mobi engineers understand the policy options presented by MDM platform, device manufacturers, and mobile OSs.
Platform Support Level	MDM platforms integrate with every critical data system in your organization. Whether on-premise or in the cloud, a stable, secure MDM platform safeguards your organization from the thousands of entry points your mobile footprint creates.

Asset Access Level	It takes many hands to support a global mobile workforce or clientele. In order to do so safely, Mobi engineers design each support agent's access and visibility just for their required job to be done.
Security Enforcement	All of the security in the world is ineffective if it is not enforced. Compliance policies, processes, and enforcement are a daily effort for Mobi MDM engineers.
Mobile Forensics	In the event of need, forensic capture of a device's data is available. A full forensic analysis and support is available on a project basis.

EMM Training Management

Training Management	
Admin, Tier 1, Tier 2	Training is necessary to support any deployment. Mobi engineers know that shared knowledge is best for the bumpy roads ahead. Mobi engineers consider it their responsibility to make sure all levels of user support are equipped with the knowledge necessary.
Social Training	Social sharing channels are now common. Mobi frequently utilizes social platforms to create user support groups and information dissemination.
Monthly/Bimonthly Scheduled Overseas Training	Coordinating a global support cannot be accomplished without regular, timely, communication. Mobi standard procedures establish regular call cycles to make the platform engineers available to all global support for education and communication.
Knowledge Articles	If there is one thing you can bank on with mobility, it is that it will change significantly every year. That means a lively, aggressive documentation process must be established to make sure expert knowledge is available through all channels. Mobi engineers know this, anticipate the needed changes, and are required to keep knowledge articles up to date.
User Training	Mobility is about the user. The end goal of all training is to make sure we are equipping the organization for success. High user adoption, engagement, and satisfaction are metrics we gather and use to drive how we adapt our designs for the jobs being done.

EMM Platform Management

Platform Management	
EMM Platform Load Management	Mobility brings massive spikes to network traffic far exceeding previous transactional desktop and web applications. In order to maintain a strong connection to the services Mobi engineers work with an organization's network teams to facilitate properly responsive load balancing to maximize network behavior for mobile devices.
EMM Platform Vendor Communications	Organizations rely on their software and hardware platforms to be backed by the vendors who make them. Mobi engineers work alongside vendors to facilitate break fix, issue resolution, root-cause analysis, and debugging efforts.
EMM Platform Deployment	Mobility is in a grand moment of change and adoption. Mobi engineers architect to anticipate scale weather you are just adopting an MDM platform, migrating platforms, or scaling, Mobi can deploy hosted or on-prem solutions.
EMM Platform Integration	MDM platforms integrate with all of the critical data systems in an organization in order to offer security, identity management, file services, analytics, and more. Mobi engineers have worked in enterprise infrastructure and know what it takes to integrate complex environments.
EMM Platform Updates	Nothing is in a steady state. Mobi will work with your vendors to manage platform updates, test in PoC environments, and control global production rollouts.

EMM Platform Design Planning	Planning is the key to capturing the strength of mobility. Mobi engineers help organizations know what is possible in their mobile platform of choice and how to plan for the future.
EMM Policy Build & Enforcement	The heartbeat of any MDM platform is identity and policy design. Mobi engineers design specifically for the job to be done.
EMM Configuration Optimization	Like updates, nothing sits still for long in any organization. It is Mobi's hope that a highly efficient and stable mobile platform becomes the norm for your organization. By keeping a constant eye on the small pieces of the MDM configuration we make small changes to see large results.
EMM Database Cleanup	After every update it is important to make sure your data is stable and ready. As a standard procedure Mobi engineers cleanup data after regular updates.
EMM Device/User Enrollment	Each managed mobile device has a critical touch point: the first time someone enrolls. Mobi works to make this as effortless as possible, and if something does arrise, we are there to help your users get through it.
EMM Compliance Cleanup	Typically once a month a previously agreed upon process is engaged where out of compliance devices are removed from management. This controls data for security purposes and makes sure your organization isn't paying for licences it does not need.
EMM User/Group Identity Maintenance	Identity structures are important to mobile management. As a standard practice Mobi regularly verifies identity management and writes procedures for user removal, both standard and emergency.

EMM Documentation Management

Documentation Management	
Infrastructure Design Maps	Mobi creates infrastructure maps for the environments we deploy and manage. This allows knowledge to be disseminated for strong support.
Knowledge Articles (KB construction)	Vital to support is the constant flow of knowledge articles written to reflect key changes, coming practice models, and solutions to common problems.
Communication Package Development	Mobi relies on a commitment to over-communicate to users inside the organization. By utilizing every tool available in any organization, Mobi will help create the materials necessary to keep your users informed and ready.
User Awareness Documentation	Specifically written for the end user, as a standard procedure, Mobi creates end-user specific material intended to guide even the most novice of users into a healthy relationship with the organization's mobility goals.

EMM Application Management

Application Management	
Application Deployment	Mobi engineers work with internal or external development teams to publish, distribute, and version specific applications key to the organization.
Application Group Assignment	Mobi designs application management and distribution specifically for the intended target. A strong identity management schema provides clear application targets.
Application Repository Management	Mobi engineers create application repositories in case a previous version is needed or if applications are not ready for production or staging.
Application Planning/Use Analytics	Mobi engineers will work with application dev teams to help provide development planning and valuable analytics.
Application Security Policy Design	Security has many layers, some of which occur inside of the application and some inside of the MDM platform. Mobi engineers will work to help you decide what is most important for your goals, then design and manage application security.

EMM Update Management

Update Management	
Update Repository Management	An update repository makes sure you never lose a critical software asset. As a standard procedure Mobi engineers stand up and maintain an update repository.
PoC Environment Management	As a standard practice a proof-of-concept environment, meant to reflect the organization's production environment, is stood up. It is used to accomplish updates and test against them. Challenge vendor claims and make sure nothing gets into your production environment without at least kicking the tires first.
Update Planning	Updates to platforms or applications require a special set of efforts. Mobi engineers will work across teams to make sure key stakeholders know what is coming and when they can expect to see it.
Post Update Testing	Mobi engineers will test every platform update that is intended for your environment. Although we certainly can not test every possible event, we will always be familiar with what is happening and what the strength and weaknesses are of the new update.
Device Synchronization Planning/Testing	Mobi will anticipate OS updates with platform testing to anticipate issues relative to manufacturer release. This will enable a smoother operations and user experience across the organization.

3. Scope of Services

MOBI will provide Mobile Device Management Services (called "MOBI MDM" or "MDM Services"), as identified in this Service Attachment. MOBI MDM is a service that helps organizations design, implement and manage an Enterprise MDM Deployment. It is compromised of platform implementation, platform migrations, platform management, platform update management security management, application management, Sr. Level support, and vendor support.

4. Support

MOBI will act as the single point of contact for Sr. Level support of the MDM platform and escalated Subscribing Entity issues. Escalated issues would route via the dedicated Account Specialists and would be the customer-facing group.

All transactions will be managed and tracked within the MOBI portal to provide centralized reporting on system activity and support metrics.

5. EMM Management Scope

MOBI Enterprise Mobility Management support for Air-Watch is composed of the following scope. All the items listed below are ongoing support and are part of the overall support. There is no cap or additional charge for performing these functions on a regular basis.

The State SaaS Server

a) Configure/Update/Review policies & processes
b) Configure/Update/Review configurations, setting, relationship structures
c) Assess overall health of Server
d) Configure/Update/Review server and infrastructure components
e) Configure/Update/Review infrastructure vulnerabilities & opportunities
f) Optimize overall current state
g) Suggestions for improvements
h) Evaluate Upgrades and Provide risk assessment
i) Perform Sever Upgrades
j) Implement/Build new Servers
k) Monitor Server
l) Manage Admins, Device Based Access, Admin Accounts RABC
m) Provide API Integration to the Mobi Portal
n) Manage/Optimize Policies and Configurations
o) Manage Apple DEP
p) Manage/Optimize Settings (SEG,ACC, LDAP, CA, Connector)
q) Manage Certificates
r) Manage registration Templates
s) Manage Update Applications
t) Assess/Troubleshoot/Escalate Core issues to Air-Watch on behalf of Subscribing Entity

SEG Server (Secure Email Gateway Service – Owned by the State)

a) Implement/Build SEG Servers
b) Evaluate SEG Upgrades and Provide Risk Assessment
c) Upgrade SEG Server
d) Configure SEG Server for ActiveSync
e) Configure SEG Server for AppTunnel
f) Configure SEG Server for Kerberos Authentication
g) Monitor SEG Servers
h) Assess/Troubleshoot/Escalate SEG issues to Air-Watch on behalf of Client
i) Troubleshoot Logs and Issues with ActiveSync

Enterprise APP Store

a) Support Enterprise App Store
b) Install/Upgrade Applications
c) Test application deployment
d) Application Functional Testing
e) Support MDM issues and Dev Team (Third Party or In-house)

Secure Content Locker

a) Install/Configure/Manage SCL Configuration and Policies
b) Support Email Attachment Controls
c) Support Repository Access (O365, SHPT, CIFS)
d) Configure Tunneling Configurations
e) Support/Configure Content Sync
f) Support/Configure CSS

6. Ongoing Operational Platform Support

MOBI Enterprise Mobility Management Services will assume ongoing support of the State's MDM platform.

7. Operational Support Scope

A. Remotely Administer existing/new MDM platforms via secure VPN

B. Perform Tier 2, Tier 3 and Sr. Support

C. Maintain Technical Support Documentation

D. Perform Management of Platform DEV and/or QA Servers

E. Perform Server software updates and testing of updates

F. Perform Device Operating System Testing

G. Perform Device Testing for Production Use

H. Validate Operating Systems for Production Use

I. Perform Security Management – Creating, Updating and reviewing policies for optimization

J. Perform Configuration Management - Creating, Updating and reviewing configurations for optimization

K. Provide Policy/Configuration review and reconciliation results to client

L. Deploy Policy and Configuration Settings as approved by client

M. Perform MDM Technical Support Maintenance

N. Perform MDM-related activities in-line with MOBI mobility triggers, including:

   a. Push approved applications;

   b. Remote device lock;

   c. Perform enterprise wipe;

d. Enroll / un-enroll users;

e. Push profiles to devices;

f. Produce MDM reports;

O. Perform MDM-related activities in-line with support events, including:

a. End User support during initial MDM set up;

b. End User ongoing troubleshooting and support via MDM environment;

c. Email configuration and recovery;

d. Profile pushing and re-pushing to support users; and

P. Perform Application Management – Limited to Installation to the MDM platform, distribution to the corporate app store. Scope does not include Application Development

Q. Perform Application Testing – Limited to distribution of the application to the App store, Installation on devices and opening of the application. Scope does not include general testing of application functionality.

R. Perform Application Distribution Configurations – Creating/Utilizing groups for application distribution. (i.e. Finance users get an ERP application)

S. Perform Training of dedicated support staff

T. Perform Platform Load Management and Optimization

U. Perform Monthly Compliance Cleanups

V. Perform Root Cause Analysis of Escalated issues

W. Perform Server availability monitoring for up/down status

X. Conduct periodic security revalidation review of platform and administrative procedures comply with client security requirements

Y. Perform Vendor MDM application testing – Scope includes full functionality testing of the application

Z. Configure and deploy vendor containerized solutions (if applicable to deployment)

AA. Configure and deploy vendor secure applications (if applicable to deployment)

BB. Configure and deploy vendor secure document solutions (if applicable to deployment)

CC. Perform Vendor container solution testing (if applicable to deployment)

DD. Perform Vendor secure application testing (if applicable to deployment)

EE. Perform Vendor content delivery testing (if applicable to deployment)

FF. Create and maintain a suite on Platform test cases

GG. Perform Change Management in cooperation with Customer procedures

8. STATE OF OHIO Responsibilities

- Provide a Point of Contact for each Agency for Requests
- Administrative Access to MDM Console and MDM related servers such as ACC and/or SEG Servers

Service Level Agreements (SLA)

9. Equipment and Software Covered

This SLA covers only the equipment, software and services as stated below.

MDM Infrastructure - All Servers in the MDM Infrastructure are covered under this Service Attachment. This includes DR servers, QA and DEV Environments.

Services – All Services are defined in the quote that will be attached to each Order.

STATE OF OHIO is responsible for any hardware acquisition for the above stated environments, if applicable.

10. SYSTEM & SERVICE MAINTENANCE

Scheduled Maintenance (Expected downtime)

Infrastructure maintenance is scheduled per the dates in the Change control system. All business approvals are granted before proceeding with any server maintenance.

Security Maintenance (Expected downtime)

This state is only encountered when MOBI detects or is alerted to urgent or critical security vulnerability. The security of client systems is of upmost priority to MOBI. Mobi works with business and security teams to determine the risk level and course of action.

Emergency Maintenance (Unexpected downtime)

In the event of a system failure, Mobi engineers will assess, open and IRT and work a course of action that has systems back online

11. <u>Guaranteed Response Times</u>

Response time is measured by how long it takes the supplier to accept, respond and resolve a request raised within the desired service management system.

Guaranteed response times depend on the priority of the service now incident. Response times are defined in the table below:

Incident SLA's		
Priority	Acceptance SLA	Completion SLA
Priority 1 Incident (Urgent)	30 mins	1 Hour
Priority 2 Incident(High)	2 Hours	4 Hours
Priority 3 Incident(Normal)	1 Business Day	3 Business Days
Priority 4 Incident(Low)	2 Business Days	5 Business Days

Prioritization Matrix

The Prioritization Matrix reflects the Impact and Urgency level combinations and the resulting Priority

Priority		Impact		
		High	Medium	Low
Urgency	High	1 – Critical	2 – High	3 – Medium
	Medium	2 – High	3 – Medium	4 – Low
	Low	3 – Medium	4 – Low	5 – Low/Planning*

- **Impact**: the effect on business that an incident has
- **Urgency**: the extent to which the incident's resolution can bear delay
- **Priority**: how quickly the service desk should address the incident

***Note:** Priority 5 incidents can be handled either as Priority 4 incidents or as a different category (Planning? ITIL) of incidents if they don't need to be resolved under specific SLAs*

Business Impact	Definition
High	Business critical configuration item or Service. Configuration items or Services that if unavailable or degraded would negatively impact product availability, patient safety, external financial or regulatory reporting, data integrity, compliance with internal policy.
Medium	Configuration items/Services that if unavailable or degraded would negatively impact business operations.
Low	All Configuration items/Services not classified as Medium or High Business Impact.

Urgency	Definition
High	• Incident/Problem that impacts multiple users in multiple locations and Service is not available for normal business operations. • Incident/Problem impacts multiple users in a single location
Medium	• Incident/Problem impacts a Premier or Enhanced User
Low	• Incidents/Problems not classified as Medium or High Urgency

12. Exclusions

MOBI will always do everything possible to rectify every issue in a timely manner. However, there are a few exclusions. This SLA does not apply to:

- Any equipment, software, or other parts of the IT system not mentioned above.
- Any services outside of the Service Attachment.
- Hardware procurement.
- Device Procurement.

Additionally, the SLA does not apply when:

- The problem has been caused by using equipment, software or service(s) in a way that is **not recommended**
- The client has made unauthorized changes to the configuration or setup of effected equipment, software, or services
- The client has prevented MOBI from performing required maintenance and update tasks
- The issue has been caused by unsupported equipment

As per the MSA, these SLAs do not apply in circumstances that are beyond MOBI's control or if Subscribing Entity is in breach of contract for reasons as stated in the MSA.

13. Fee Schedule

See Addendum A

In Witness Whereof, the Parties have executed this Amendment, which is effective on the date the State's duly authorized representative signs it on behalf of the State, ("Effective Date").

MOBI		**STATE OF OHIO, DEPARTMENT OF ADMINISTRATIVE SERVICES**
James Hamstra		Robert Blair/SRO
Signature		Signature
James Hamstra		Robert Blair
Printed Name		Printed Name
Corporate Counsel		DAS Director
Title		Title
September 12, 2017		9/19/17
Date		Effective Date
26-3812495		
Federal Tax ID		