Synoptek { Mobile Device Management

TABLE OF CONTENTS

INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Mobile Device Management (the "Service").

The Service Definition found herein reflect Synoptek standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect Synoptek's best practices or industry standards at its sole discretion with or without notice.

1.1 SERVICE SCOPE

2 SERVICE OFFERINGS

This service provides you (Customer) with a comprehensive enterprise mobility management solution. This service enables your employees to maximize productivity by managing your workforce's mobile devices to ensure secure enterprise access on the go. It serves to protect and manage your corporate and personal devices.

The service includes Mobile Device Management (MDM), Mobile Application Management (MAM), and a Container App to offer enhanced application and performance management over mobile devices. Synoptek will provision the software for customer. Synoptek will set policies, as well as configure email, calendar, contacts, Wi-Fi and VPN profiles in order to quickly onboard users. Due to the nature of "Bring Your Own Device" classified devices, Synoptek is not accountable nor responsible for ensuring compliance with software and associated policies as it relates to these devices. Post-launch of the service, Synoptek will provide support with respect to the adjustment of device and application policies as requested by the Customer.

Note: *Synoptek will support applications that come with MDM and the policies that come with these services. Synoptek will not support hardware, OS, and carrier related issues.*

The service is priced per device. Users with multiple devices will charged an additional fee accordingly.

2.1 STANDARD COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED

MOBILE DEVICE MANAGEMENT	Synoptek will manage Customer's mobile devices using MDM software designed for smartphones and tablets. The software used will support iOS, Android, and Windows devices as specified in Appendix 6.2.
	
	Synoptek will manage Customer's mobile devices as requested by Customer needs and policies, as well as manage any changes to implemented policies as requested by the customer post-launch.
	
	The detailed list of what Synoptek will manage is as follows:
	• Enrollment of mobile devices (bulk enrollment, link via text message or email)
	• Integration with enterprise systems (Microsoft Exchange and Office 365)
	• Configuration management:
	  • Configuration of email, calendar, contacts, Wi-Fi and VPN profiles.
	• Restricted access based on geolocation
	• Restriction of camera and screen capture functionality
	• End user support:
	  • Password reset and remote control
	• Compliance and enforcement:
	  • Application of tailored security policies for specific devices or personas that span across devices.
	  • Enforcement and provisioning of passcode and encryption policies
	  • Detection and restriction of jailbroken and rooted devices.
	  • Remotely locate, lock and wipe lost or stolen devices; selectively wipe corporate data while leaving personal data intact.
	• Monitoring and reporting:
	  • Self service mobility intelligence dashboards allow customers to gain a graphical summary of operations and compliance.
	  • Detailed hardware and software reporting are available upon request, but not set up by default.
		Yes

	• Bring-your-own-device (BYOD) privacy settings are used to block collection of personally identifiable information.	
MOBILE APPLICATION MANAGEMENT	Synoptek will securely manage applications used by Customer's workforce across all devices supported by this service using an enterprise application catalog with built-in security and operational lifecycle management capabilities. Synoptek will manage and distribute up to maximum of 10 applications to a maximum of 5 user groups as well as set and enforce compliance policies: • Definition of required, whitelists, and blacklisted apps • Restriction for native applications, jailbroken/rooted devices, and network access • On-device access control and automated compliance measures • Additionally, Synoptek will manage patch and update management for compliant devices. Furthermore, Synoptek will service device wipes with the following extents: • Full device wipes: Customer-owned devices only • Selective device wipes: Personal and customer-owned devices Synoptek will manage Customer's applications as requested by Customer needs and policies, as well as manage any changes to implemented policies as requested by the customer post-launch.	Yes
VCISO	Customers with specific compliance needs may request Synoptek to provide additional resources for Security Planning to ensure customer meets industry regulations. See vCISO Service Definition for further information.	Optional Service – Additional Charges Apply

2.2 PREMIUM COMPONENTS

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
SECURE MOBILE MAIL	Synoptek will include and manage a separate, secure office productivity application for users to manage email, calendars, and contacts. This includes the following data loss prevention measures:	Deluxe

	• The ability to contain and control the flow of emails and attachments • Authentication enforcement • The ability to restrict copy/cut/paste & forwarding • The ability to lock down documents to view-only mode FIPS 140-2 compliant, AES-256 bit encryption for data at rest (data stored on a device, not currently being transmitted across a network) can be used as well.	
SECURE MOBILE CHAT	Synoptek will provide and manage a mobile chat application for Customer's workforce to communicate in a secure, corporate-sanctioned environment. This includes the following security measures: • Containment of all chat conversations and data within a passcode-protected workspace, separated from personal data • Familiar, easy to use chat interface that enhances collaboration and productivity • Copy/paste restrictions • Corporate directory lookup to establish quick connections • Availability view of contacts • Notifications for newly initiated one-on-one and group conversations • Optional display of conversation history	Deluxe

3 SERVICE DEPLOYMENT

3.1 EXPECTATIONS DURING ONBOARDING

3.1.1 Synoptek Requirements:

- Synoptek will require the following of the customer during onboarding:
  - An Active Directory-connected server to be used as a cloud extender for AD related integration
  - A review of the iOS and/or Android data collection form with the customer:
    - For the purposes of building out the policies/restriction/settings – to meet the customers' requirements
  - User Acceptance Testing (UAT) group for testing the policies/restriction/settings
  - A list of the users and their devices type (IOS or Android) for proper enrollment of the clients

3.1.2 Synoptek Deliverables:

- Synoptek will deliver the following to the customer after requirements (above) have been met:
  - Buildout of the customer in MaaS360.
  - Installation and configuration of the Maas360 Cloud Extender on a customer AD connected server
  - Buildout of the policies/restriction/settings with MaaS360 – to meet the customers' requirements
  - User Acceptance Testing (UAT) of the policies/restriction/settings and any required adjustments (tweaking)
  - Send out enrollments to the user base and reporting to the customer on enrollment progress
  - Send out enrollment instruction documentation to the customer.
  - Send out further documentation on Secure Mobile Mail, if applicable.

3.2 ONBOARDING TIMELINE & TRANSITION TO SUPPORT

- Build-Out Timeline: Varies, depends on the following:
  - Customer Requirements. The length of onboarding/build-out will depend on the complexity of the build out and customer requirements.
  - User Enrollment. Synoptek does not push the client out, end user involvement is required.
    - Synoptek will give end users 2 weeks to accept the enrollment.
    - At the end of this time frame, Synoptek will report enrollment progress to customer.
    - Customer will then have the option to send out further correspondence to end users if desired.
    - Once the above actions are completed, Synoptek will complete a true up and the number of users will be adjusted, as needed.
- Upon completion of User Enrollment activities, and the final user count is determined, billing will begin.
- Upon completion of QA the customer will be transitioned over to support.

4 SUPPORT

The service and support operate 24x7x365. As the owner of the issue, Synoptek will log, track and isolate the problem, and either resolve the issue or escalate it to the appropriate service provider designated by Customer or to Customer's internal support group.

4.1 SERVICE LIMITATIONS

Although this Service serves to improve the management capability of mobile devices, and has security components, your organization retains ultimate responsibility for all risks and liability of mobile devices, including "Bring Your Own Device" classified devices.

The Service described is not synonymous with roles such as:

- Mobile Device Security
- Mobile Device Incident Response

4.1.1 Exclusions; Unsupported Incidents:

- These services are not intended as consulting, design or implementation services. The following items and functions are not supported under the Service:
  - The administration of Customer's systems (including server on-boarding (set-up), server off-boarding (decommission), and enterprise server configuration changes unless otherwise noted in this service definition); on-site desktop support; device setup; data backup and file restoration; printer RMA issues; smartphone, PDA and tablet applications; and devices and applications not provided by Synoptek as part of the Service or specifically identified in a Statement of Work ("SOW") signed by the Parties.

4.1.2 Communication of Out-of-Scope Issues.

- Out-of-scope issues identified by Synoptek will be documented and communicated to the Customer.
- The Customer will be responsible for management of its systems and must work directly with its manufacturer or vendor for assistance with unsupported, third-party applications and devices.
- The Customer also is responsible for failures caused by viruses, user abuse, environmental conditions and other causes not within Synoptek's control.
- Out-of-scope issues can be remedied with Synoptek Professional Services on a time and material basis.

4.2 REQUIREMENTS FOR THIS SERVICE

The following specifications are required for Synoptek's Mobile Device Management Service:

- The software deployed by Synoptek to customer devices should not be tampered with, and user profiles should not be deleted by Customer.
- The Customer must call in to Synoptek with any support requests, incidents, requests, or changes, in order to receive appropriate service and support.
- The Customer must follow set processes, as necessary, regarding any changes.
- The Customer must notify Synoptek regarding any devices that need to be removed from management.
- The system being covered under this Service must be officially supportable by the device and OS manufacturer for the life of this Service Order, i.e. must not be EOS (End of Support).

Customer acknowledges and agrees that Synoptek may directly or remotely communicate with the agents we install on Customer's Devices for purposes related to the security and management, including, (i) verifying Credentials; (ii) issuing reports and alerts such as automated support requests and alert messages; (iii) providing support and maintenance

services; (iv) applying policy and configuration changes; and (v) extracting usage information, service performance information and event logs.

4.3 SYNOPTEK RESPONSIBILITIES

- Synoptek can provide reporting on devices and associated data. Synoptek will require the following to do so:
  - Specific components to report on, scheduled interval of the report (weekly, monthly, etc.), and an email address for Synoptek to send report to, once generated.

4.4 CUSTOMER RESPONSIBLITIES

- The Customer is responsible for securing and managing their own device support contracts with a 3rd party carrier.
  - This includes the management of 3rd party vendor mailboxes, data plans, associated hardware, and any other aspects of device management not included in the scope of services defined above.
- The Customer must not perform any action on the System which would interfere with Synoptek's ability to monitor or manage the Service including, but not limited to the following actions:
  - Disabling or changing any user or service login accounts used by Synoptek for monitoring or managing the System
  - Removing or changing any monitoring agent software settings
- The Customer is responsible to notify the Service Desk (Support@Synoptek.com) when affecting the System, or when performing any other activity which would result in an "outage" as seen from the monitoring system.
  - As security is application-dependent, the Customer is responsible for the overall security of applications and data. Synoptek is not responsible for the security or the integrity of software or data installed on the System or any applications which it is running.

4.5 CHANGE MANAGEMENT

The Synoptek approach to change management is to ensure that all changes are implemented with minimal impact to existing services and applies to any proposed alterations to existing IT services or the IT environment.

5 OPTIONAL SERVICES

5.1 Virtual CISO (vCISO)

For customers that must comply with strict regulations (HIPAA, FINRA, HITRUST, ISO, SOX, etc.), Synoptek recommends use of this optional service. See the vCISO Service Definition for further information.

5.2 DESIGNATED CONSULTING ENGINEER (DCE)

For customer application management, Synoptek offers Designated Consulting Engineers. These resources will work remotely and are scheduled in advance for a set number of hours per month.

6 APPENDIX

6.1 ADDITIONAL NOTES ABOUT SERVICE COMPONENTS

In reference to Section 2.1 Essentials Components: Mobile Application Management: Synoptek can perform full device wipes on corporate owned devices ONLY. Synoptek can perform selective wipes on both corporate devices and personal devices. Synoptek will only deliver *business related* applications to users and user groups.

Comparison Chart: Corporate vs. Personal Devices		
	Corporate Owned Devices	Personal Devices
Full Device Wipe	✓	X
Selective Wipe	✓	✓

6.2 SUPPORTED DEVICES

Supported Device Types and OS Versions		
iOS	**Android**	**Windows Phone 8+**
iOS 5.x (iPhone, iPad)	Android 2.2+	Windows Phone 8 and Windows Phone 8.1
iOS 6.x (iPhone, iPad)	Android 3.x	Windows Phone 10 versions (1511, 1607, 1703, 1709)
iOS 7.x (iPhone, iPad)	Android 4.x	

iOS 8.x (iPhone, iPad)	Android 5.x	
iOS 9.x (iPhone, iPad)	Android 6.x	
iOS 10.x (iPhone, iPad)	Android 7.x	
iOS 11.x (iPhone, iPad)	Android 8.x	
iOS 12.x (iPhone, iPad)	Android 9.x	

6.3 COMPARISON CHART: MDM SOLUTIONS

Comparison Chart

Mobile Device Management	MDM Standard Suite	MDM Premium Suite
Mobile Device Management		
Smartphones and tablets	✓	✓
Email, calendar, contacts, Wi-F and VPN configuration	✓	✓
Device Feature Restrictions (camera, screen capture, cloud backup, etc.)	✓	✓
Granular Security Policy Setting	✓	✓
Remote location, lock, or wipe of devices	✓	✓
Monitoring and Reporting Capabilities	✓	✓
Mobile Application Management		
End User App Catalog & Discovery Portal	✓	✓
Mobile Application Lifecycle Management		
Build out 10 apps and deliver to 5 user groups per customer*	✓	✓
Compliance and Enforcement		
Blacklist, whitelist, and set required apps	✓	✓
Restrict access for jailbroken or rooted devices	✓	✓
Enforce on-device access control & automated compliance with policies & regulations	✓	✓
Container App		
MaaS360 Agent app	✓	✓
Secure Mobile Mail		
PIM capabilities such as Mail, Calendar, and Contacts		✓
Secure Mobile Chat		
Secure, corporate sanctioned instant messaging		✓
Containment of all chat conversations and data		✓
Availability view of contacts		✓

**This is the set number of allowed apps and user groups. If limits are exceeded, additional charges may apply.*