

Service Attachment # 1

This Service Attachment (the "Service Attachment"), is between Air Watch ("Service Provider") having an office at 145 E. Superior St. Atlanta, GA, and the State of Ohio, Department of Administrative Services, Office of Information Technology ("the State"), having its principal place of business at 1320 Arthur E. Adams Drive, 3rd Floor, Columbus, OH 43221 (jointly referred hereto as the "Parties"), and it is effective as of the date signed by the State. It amends that certain Master Cloud Services Agreement between the Parties dated 5/4/2012

1. Definitions.

The defined terms in the Master Cloud Services Agreement ("the Agreement") and the End User License Agreement attached thereto ("the EULA") will have the same meanings in this Service Attachment as they do in the Master Cloud Services Agreement. There may be additional definitions contained herein.

2. Software.

- **Overview.** Service Provider is providing a SaaS License for the AirWatch SaaS Mobile Device Management that includes the Secure Email Gateway and the Secure Content Locker. AirWatch Mobile Device Management software solution provides mobile security, device, application, and content management across multiple smartphone and tablet computer platforms. 24x7x365 maintenance and support is included for the AirWatch Mobile Device Management software solution SaaS License Fee.

- **Standard Software Features.**

- **Device Support**

- AirWatch supports the following Mobile OS / Platforms:
- Apple iOS: 3.x, 4+, 5+
- Android: 2.2+
- Windows Mobile: 5+
- Blackberry: 4.5+
- Symbian: Symbian^3 and S60+
- Some Windows 32 manufacturers
- Devices running Windows CE: 4,5, 6
- Windows Phone 7+

- **Mobile Device Management Phases**

- **Enroll**

- Device Ownership: Enroll employee, corporate or shared devices in your enterprise environment
- Device Staging: Allow IT administrator to stage devices on behalf of other users to simplify enrollment
- Device Registration: Enable IT to register existing devices in bulk or end users to self-register their device
- User Authentication: Authenticate users via basic or directory-based authentication (Authentication can be done via AD/LDAP, SAML or tokens)
- EULA: Create custom End User License Agreements (EULAs) and require acceptance during enrollment
- Restrictions: Set up enrollment restrictions to block users or devices based on platform, version, etc.

- **Secure**

- Passcode: Require a device passcode with configurable complexity, length, lock and wipe rules

Service Attachment # 1

- **Encryption:** Enforce full device and storage card encryption according to industry standards
- **Compliance:** Set up rules for non-compliant activities and compromised devices with automated responses
- **Configure**
 - **Profiles:** Configure device settings and user credentials for accessing enterprise resources
 - **Certificates:** Integrate with certificates for secure distribution and management of profiles
 - **Accounts:** Provision access to corporate Email, Calendar, Contacts, Wi-Fi and VPN networks
 - **Applications:** Distribute and manage internal/public/purchased apps via the App Catalog
 - **Content:** Distribute corporate documents and secure mobile access using Content Locker
- **Monitor**
 - **Privacy:** Configure what data is collected and who can view it for different device groups
 - **Dashboard:** Track and view real-time device information via interactive dashboards and portlets
 - **Alerts:** Create event alerts with automated routing policies to notify IT administrators or end users
 - **Rules Engine:** Set up rules that define non-compliant events/activities and automated responses
 - **Reporting:** Export data directly from the dashboard or generate reports with automated distribution
 - **Data Mart:** Import device data to enterprise BI tools
- **Manage**
 - **Queries:** Determine the frequency intervals at which the console captures device information
 - **Updates:** Update configuration profiles on-demand and re-provision devices automatically
 - **Commands:** Send commands on-demand to devices to request info, lock or wipe a device
 - **Retirement:** Un-enroll devices from your environment, remove corporate data and wipe device
- **Support**
 - **Messaging:** Send a customized message to end users with troubleshooting instructions
 - **Remote Diagnostics:** Perform remote diagnostics to identify device issues in real-time
 - **Commands:** Send commands on-demand to devices to request info, lock or wipe a device
 - **Remote View:** View an end user's device screen and take screen captures
 - **Remote Control:** Take remote control of an end user's device for troubleshooting
 - **Self-service:** Enable end users to clear their passcode, locate their device and more
- **Mobile Device Management Phases**
 - **Application Distribution**
 - Distribute managed (enterprise) apps wirelessly without user interaction
 - Integrate directly with public app stores, like Apple, to provide public apps

Service Attachment # 1

- Integrate with Apple's Volume Purchase Program to purchase business apps
- Secure distribution of apps based on groups with unique requirements and access
- Provide an enterprise app catalog where users can view, install and update apps
- **Application Security**
 - Authenticate users before allowing them to view and download enterprise apps
 - Secure access to the enterprise app catalog based on user role or device function
 - Restrict native apps on a device and whitelist/blacklist publicly available apps
 - Monitor and enforce device compliance with corporate application policies
- **Application Tracking**
 - Set privacy policies for the app data that is collected based on device ownership
 - Track and view installed/approved/rogue applications at the device/user level
 - Receive instant alerts when an end user has installed an unapproved app
 - Generate application inventory, version history, and compliance reports
- **Application Management**
 - Configure corporate policies for public apps using whitelists and blacklists
 - Install, update and remove managed apps from a device remotely
 - Disable access to corporate apps if an end user leaves or loses their device
- **Integration with Apple's Volume Purchase Program**
 - Track VPP orders, including order date number, status and more
 - Monitor licenses purchased, redeemed and remaining for each order
 - Associate orders to a purchase order number, department, or cost center
 - Upload, store and distribute redemption codes to authorized users
 - Confirm the redemption of codes and successful installation of apps
 - Associate redemption codes/licenses to users and devices in the system
- **Software Development Kit (SDK) for Enterprise Apps**
 - User authentication with Directory Services and Certificates integration
 - Over-the-air app distribution and updates without user interaction
 - Device & app information and usage monitoring
 - Compromised device detection with automatic wipe capabilities
 - Passcode enforcement with ability to lock access after failed attempts
 - Encryption for data in transit and data stored within an enterprise app
 - Remote wipe of app data based on non-compliance or on-demand
- **Mobile Content Management**
 - **Enterprise-grade Security**
 - Authentication: Authenticate users via basic or directory services-based authentication
 - Encryption: Transmit documents over industry standard 256-bit SSL encrypted connections
 - Compliance: Require devices to be compliant with corporate policies or enrolled in MDM
 - Access: Disable access or perform a device wipe if the device is compromised or non-compliant
 - Sharing: Control user's ability to edit, share or open files in unauthorized applications
 - **Cloud Content Management**
 - Store documents in a cloud-based content management console
 - Upload documents individually or bulk import

Service Attachment # 1

- Support multiple document types: Office, iWork, PDF, JPG, etc.
- Organize content using custom document categories and metadata
- Capture information on author, description, notes, keywords, etc.
- Track document versions and update history
- View which users have downloaded a file and when it was last viewed
- **Secure Document Distribution**
 - Publish files and updates to a single device or a group of devices
 - Enable documents to be downloaded automatically or on-demand
 - Define effective and expiration dates for each document
 - Define settings for document transfers over cellular or Wi-Fi networks
 - Set the priority level in which a file will download in the document queue
 - Enable users to view documents offline or only while online
- **Easy Mobile Access**
 - View organized content through custom categories
 - Browse via smart views: All, New, Recent, Favorites
 - Search content based on specific keywords
 - Store approved content for offline viewing
 - Receive automatic updates and notifications
- **Mobile Content Management (for the Secure Content Locker)** includes 5GB of storage for the State of Ohio.
- **Optional Software Features.**
 - Beyond the initial 5GB of storage provided with Secure Content Locker, additional blocks of storage for Secure Content locker in increments of 25GB are available for \$5 per month.

3. Provision of Software. The Service Provider will make the Software available to the Subscribing Entities pursuant to the Agreement, this Service Attachment, and the applicable order made pursuant to the State's TRS System. The State agrees that purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by the Service Provider regarding future functionality or features.

4. The Service Provider Responsibilities. The Service Provider must: (i) provide the Service Provider's basic support for the Software to State at no additional charge (such charges being included in the SaaS License Fees), and/or upgraded support if purchased, (ii) use commercially reasonable efforts to make the Software available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which the Service Provider must give at least 8 hours' notice via the Software and which the Service Provider must use commercially reasonable efforts to schedule between 10 p.m. and 6 a.m. Eastern Time and on Saturdays, or (b) any unavailability covered by the EULA's Excluded Event clause or by the Service Level section later herein, and (iii) provide the Software in full accordance with applicable laws and government regulations.

5. Fees and Payment

- **Fee Structure**
 - **Nitrodesk Touchdown** will be provided at no charge to the State of Ohio for Android devices that AirWatch does not yet configure settings for the native mail client. Today AirWatch can configure the native mail client for Samsung SAFE devices such as the Galaxy Note and Tab 7.7.
 - **SaaS License Fees** AirWatch per unit pricing for the State of Ohio is based on an expected order quantity of licenses for 2,700 Devices..

Service Attachment # 1

<u>Product Code</u>	<u>Product description</u>	<u>Unit Price</u>	<u>Discount %</u>	<u>Net Unit</u>
MDM-SB-SD	SaaS License Subscription – MDM	\$3.00	21%	\$2.37 / Month
MCM-SB-SCL	SaaS License Subscription-Content Locker Module	\$1.00	100%	\$0.00 / Month
MDM-SB-SEG	Hosted Subscription- Secure Email	\$.75	100%	\$0.00 / Month
MDM-LF-TD	Nitrodesk Touchdown One Time Fee	\$15.00	100%	\$0.00 / Month

Note: MDM-SB-MDM is a prerequisite to order MDM-SB-CL, MDM-SB-SEG or MDM-LF-TD (%)

- o **SaaS License Fees Discount.** A discount will be applied to the monthly SaaS License Fees based upon the number of Devices under license and the following discount tiers:

- 1000 to 2499 licenses = 16% discount
- 2500 to 4999 licenses = 21% discount
- 5000 to 9999 license = 26% discount
- 10,000 or more licenses = 31% discount

- o **Professional Services** will be provided on a fixed cost basis for either (a) configuring and supporting the deployment of AirWatch Secure Email Gateway and Enterprise Integration services for a single agency within the State of Ohio existing SaaS environment or (b) configuring and supporting the initial setup and deployment of the AirWatch platform using the AirWatch Hosted SaaS platform for the State of Ohio consolidated environment. The fixed costs for both options are attached as exhibits hereto.

- **Fees.** The Subscribing Entities will pay all fees specified in the applicable order made pursuant to the State's TRS System, subject to the terms of the Agreement and the EULA. Except as otherwise specified herein or in the applicable order made pursuant to the State's TRS System, fees are based on the number of Devices under license and cannot be decreased during the relevant subscription term stated on the Order Form, except as provided in the Agreement. The SaaS License Fees are based on monthly periods that begin on the Delivery Date of the Software and each monthly anniversary thereof; therefore, SaaS License Fees for Devices added in the middle of a monthly period will be charged for that full monthly period and the monthly periods remaining in the subscription term. Additions of Object subscriptions during a term does not extend that term. No Order Form may specify a subscription term not identified and priced in this Attachment. Nor may it cover any billable services not listed in this Service Attachment as a Service.

- **Disputes.** After 90 days, the Service Provider may suspend the delinquent Subscribing Entity's access to the Software until all delinquent amounts are paid, notwithstanding the prohibition against self-help provided for elsewhere in the Agreement, but the Service Provider may not do so if the State is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute; *provided, however*, this provision shall nevertheless apply to delinquent undisputed payments.

- **Invoicing and Payment.** Fees will be invoiced monthly in arrears and otherwise in accordance with the Order Form and the Agreement. Fees are due in accordance with the terms of the Agreement, which no Order Form may alter. The State is responsible for providing complete and accurate billing and contact information to the Service Provider and notifying the Service Provider of any changes to such information.

6. Proprietary Rights. The proprietary rights of the Parties shall be governed as provided in the EULA and the Agreement.

7. Service Levels

- **SLAs for the Services.** The EULA includes SLAs that will be used to monitor and manage the performance of the Software. The minimum SLAs are listed in the EULA, but the Service Provider may

Service Attachment # 1

supplement them with additional SLAs that are generally applicable to its other Services customers, so long as those additional SLAs cover parameters not addressed in the SLAs in the EULA or are more stringent than those in the EULA. Modifications to the SLAs provided below may only be made by the written agreement of the State and the Service Provider, except with respect to SLAs the Service Provider offers generally to other customers that are more stringent or in addition to those in the EULA.

- **Availability.** "Availability" or "Available" has the same meaning ascribed thereto in the EULA.
- **Scheduled downtime.** The Software may be inaccessible to a Subscribing Entity's users during scheduled downtimes. The Service Provider will use commercially reasonable efforts to: (i) schedule downtime between 10 p.m. and 6 a.m. Eastern Time, to limit scheduled downtime to less than two hours per event, and to limit scheduled downtime to less than four per month. The Service Provider may change the scheduled downtime to other non-business hours upon reasonable notice to the Subscribing Entity. Scheduled downtime will not be considered times when the Services are Unavailable.
- **Other Exclusions.** In addition to scheduled downtime, the following will not be considered times when Services are Unavailable:
 - Outages resulting from a Subscribing Entity's equipment or its Internet service provider;
 - A Subscribing Entity's negligence or breach of its material obligations under this Agreement; and
 - Excusable Delays, as provided for and handled in accordance with the Agreement.
- **SLA Credits.** Outage Credits shall be provided in accordance with the terms of Section 10.4 of the EULA attached to the Master Cloud Services Agreement.
 - The Service Provider must actively monitor and report to the State and each Subscribing Entity any and all Unavailability of a Service monthly, along with reasonable details regarding such Unavailability. The Service Provider also must provide each Subscribing Entity that uses the Service an Outage Credit within 30 days of the end of any calendar month in which it is verified, pursuant to the EULA, that an Outage Credit is due.
 - The applicable Outage Credit will be calculated as specified in Section 10.4 of the EULA attached to the Master Cloud Services Agreement.
 - If the Outages exceed 7 hours, 12 minutes in three consecutive calendar months, any affected Subscribing Entity may terminate any or all Orders for the Software for cause.
- **The Target Availability Level** is 99.9%, as provided in Section 6.2 of the EULA attached to the Master Cloud Services Agreement.

8. Terms and Termination

- **Term of Subscriptions.** Subscriptions commence on the Delivery Date of the Software in the applicable Order Form and continue for the subscription term specified therein. Should a Subscribing Entity elect to renew a subscription, provided this Agreement remains in effect or is renewed, the renewal will be at the Subscribing Entity's option and will be for the same or greater discount from list as the subscription being renewed and under the same terms and conditions.

9. Miscellaneous

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

SERVICE PROVIDER

**STATE OF OHIO,
DEPARTMENT OF
ADMINISTRATIVE SERVICES**

Service Attachment # 1

Dan Wardle
Signature

Stuart R. Davis
Signature

Dan Wardle
Printed Name

STUART R. DAVIS
Printed Name

Finan Dirct
Title

State CID / Asst Dir
Title

5/11/12
Date

5/14/12
Effective Date

20-4745255
Federal Tax ID

AirWatch Legal
SR
Approved

Service Attachment # 1



JOHN R. KASICH
GOVERNOR
STATE OF OHIO

Executive Order 2011-12K

Governing the Expenditure
of Public Funds for Offshore Services

WHEREAS, State of Ohio officials and employees must remain passionately focused on initiatives that will create and retain jobs in the United States in general and in Ohio in particular, and must do so especially during Ohio's continuing efforts to recover from the recent recession.

WHEREAS, allowing public funds to pay for services provided offshore has the potential to undermine economic development objectives in Ohio.

WHEREAS, the expenditure of public funds for services provided offshore may deprive Ohioans and other Americans of critical employment opportunities and may also undermine efforts to attract businesses to Ohio and retain them in Ohio, initiatives in which this State has invested heavily.

NOW THEREFORE, I, John R. Kasich, Governor of the State of Ohio, by virtue of the authority vested in me by the Constitution and the laws of this State, do hereby order and direct that:

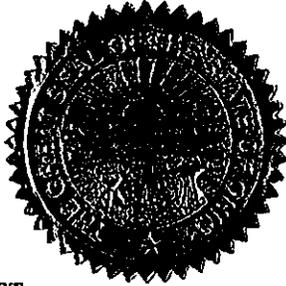
1. No State Cabinet Agency, Board or Commission ("Executive Agency") shall enter into any contract which uses any public funds within its control to purchase services which will be provided outside the United States. This Executive Order applies to all purchases of services made directly by an Executive Agency and services provided by subcontractors of those providing services purchased by an Executive Agency.
2. This Executive Order will be personally provided, by the Director, Chair or other chief executive official of each Executive Agency, to the Chief Procurement Officer or other individual at that entity responsible for contracts for services.
3. The Department of Administrative Services, through Ohio's Chief Procurement Officer, shall have in place, by July 1, 2011, procedures to ensure all of the following:
 - a. All agency procurements officers (APOs), or the person with equivalent duties at each Executive Agency, have standard language in all Executive Agency contracts which:
 - i. Reflect this Order's prohibition on the purchase of offshore services.

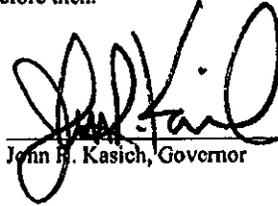
Service Attachment # 1

- ii. Require service providers or prospective service providers to:
 - 1. Affirm that they understand and will abide by the requirements of this Order.
 - 2. Disclose the location(s) where all services will be performed by any contractor or subcontractor.
 - 3. Disclose the locations(s) where any state data associated with any of the services they are providing, or seek to provide, will be accessed, tested, maintained, backed-up or stored.
 - 4. Disclose any shift in the location of any services being provided by the contractor or any subcontractor.
 - 5. Disclose the principal location of business for the contractor and all subcontractors who are supplying services to the state under the proposed contracts.
 - b. All APOs confirm that all quotations, statements of work, and other such proposals for services affirm this Order's prohibition on the purchase of offshore services and include all of this Order's disclosure requirements.
 - i. Any such proposal for services lacking the affirmation and disclosure requirements of this Order will not be considered.
 - ii. Any such proposal where the performance of services is proposed to be provided at a location outside the United States by the contractor or any subcontractor will not be considered.
 - c. All procurement manuals, directive, policies, and procedures reflect the requirements of this Order.
 - d. All APOs have adequate training which addresses the terms of this Order.
4. Nothing in this Order is intended to contradict any state or federal law. In addition, this Order does not apply to:
- a. Services necessary to support the efforts of the Department of Development to attract jobs and business to the state of Ohio;
 - b. Academic, instructional, educational, research or other services necessary to support the international missions of Ohio's public colleges and universities; or
 - c. Situations in which the Director of the Department of Administrative Services, or the Director's designee, shall determine that it is an emergency or that it is necessary for the State to waive some or all of the requirements of this Order. The Director shall establish standards by which Executive Agencies may request a waiver of some or all of the requirements of this Order and by which such requests will be evaluated and may be granted.
5. Executive Order 2010-09S is hereby rescinded.

Service Attachment # 1

I signed this Executive Order on June 21, 2011 in Columbus, Ohio and it will expire on my last day as Governor of Ohio unless rescinded before then.




John E. Kasich, Governor

ATTEST:

Jon Husted, Secretary of State

Service Attachment # 1

STANDARD AFFIRMATION AND DISCLOSURE FORM EXECUTIVE ORDER 2011-12K

Governing the Expenditure of Public Funds on Offshore Services

All of the following provisions must be included in all invitations to bid, requests for proposals, state term schedules, multiple award contracts, requests for quotations, informal quotations, and statements of work. This information is to be submitted as part of the response to any of the procurement methods listed.

By the signature affixed hereto, the Service Provider affirms, understands and will abide by the requirements of Executive Order 2011-12K. If awarded a contract, both the Service Provider and any of its subcontractors will perform no Services requested under this Agreement outside of the United States.

The Service Provider will provide all the name(s) and location(s) where Services under this Agreement will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Service Provider to sanctions. If the Service Provider will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Principal location of business of Service Provider:

1425 Ellsworth Industrial Blvd, Suite 33
(Address)

Atlanta, GA 30318
(City, State, Zip)

Name/Principal location of business of subcontractor(s): None except for data hosting centers described in in Section 4.4 of the Master Cloud Services Agreement.

(Name)

(Address, City, State, Zip)

(Name)

(Address, City, State, Zip)

2. Location where Services will be performed by Service Provider: Services will either be performed at the offices of Service Provider or on site for the State of Ohio.

Name/Location where Services will be performed by subcontractor(s): As described in in Section 4.4 of the Master Cloud Services Agreement.

Name/Location(s) where state data will be stored, accessed, tested, maintained or backed-up by subcontractor(s) are all as provided in Section 4.4 of the Master Cloud Services Agreement:

Service Attachment # 1

Service Provider also affirms, understands and agrees that Service Provider and its subService Providers are under a duty to disclose to the State any change or shift in location of Services performed by Service Provider or its subcontractors before, during and after execution of any Agreement with the State. Service Provider agrees it will so notify the State immediately of any such change or shift in location of its Services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Service Provider to perform the Services outside the United States.

On behalf of the Service Provider, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure form and have read and understand that this form is a part of any Agreement that Service Provider may enter into with the State and is incorporated therein.

By: 
Service Provider

Print Name: Dan Wind

Title: Fire Director

Date: 5/11/12


Approved

Service Attachment # 1

Project Objectives – Single Agency

This proposal includes configuring and supporting the deployment of AirWatch Secure Email Gateway and Enterprise Integration services for a single agency within the State of Ohio existing SaaS environment. The AirWatch software will be used to support device configuration and monitoring, secure mobile email and mobile application deployment.

Proposed Project Scope

Project Scope

1. Installation/Configuration of the AirWatch secure email gateway and Enterprise Integration Service in a single agency and single exchange environment.
2. Validation and testing of the devices and Email Gateway.

Deliverables: Server sizing and architecture diagrams for SEG and EIS, SEG and EIS implementation, Training documentations

Items not in scope

1. PKI Integration
2. Symbian, BlackBerry and Windows Phone 7 devices

Project Assumptions

1. All documentation and work product will be provided in English.
2. Work to be provided remotely unless otherwise specified above, or requested by the State of Ohio team.
3. Work to be performed on a fixed price basis.
4. AirWatch and State of Ohio project management will work closely together to ensure that project scope remains consistent and issues are resolved in a timely basis.

Project Costs

- AirWatch will provide the services outlined at a fixed price of **\$4,500.00**
 - Services will be billed on the following schedule
 - 50% on acceptance of the SOW
 - 50% on acceptance of all deliverables

Expenses billed as incurred according to AirWatch travel and expense policy and are the responsibility of State of Ohio for any travel needed outside the Atlanta area.

Service Attachment # 1

Project Objectives - Consolidated Environment

This proposal includes configuring and supporting the initial setup and deployment of the AirWatch platform using the AirWatch Hosted SaaS platform for the State of Ohio consolidated environment. The AirWatch software will be used to support device configuration and monitoring, secure mobile email and application deployment.

Proposed Project Scope

Project Scope

3. **Blueprint**
 - a. Assessment of the device management approach.
 - b. Planning for AirWatch Secure Email Gateway (SEG) deployment and strategy for restricting email to only managed users.
Deliverables: AirWatch MDM Framework, server sizing and architecture diagrams
4. **Prepare**
 - a. Installation of the AirWatch SEG and EIS in a single, consolidated Exchange 2010 environment.
 - b. Create and configure environment for State of Ohio in shared hosted environment
 - c. Testing and evaluation of device lifecycle in the State of Ohio environment.
 - d. Training for primary AirWatch project owners.
Deliverables: documentation of SEG and EIS environment, SEG installed, Training documentations
5. **Deploy**
 - a. Support production roll-out for up to 5 devices.
 - b. Training for extended support teams.
 - c. Provide escalation support for the State of Ohio help desk operations for any issues encountered during the initial roll out.

Items not in scope

3. PKI Integration
4. Symbian, BlackBerry and Windows Phone 7 devices
5. Integration with other Exchange and Directory environments not part of the consolidated Exchange 2010 environment.

Project Assumptions

5. All documentation and work product will be provided in English.
6. Work to be provided remotely unless otherwise specified above, or requested by the State of Ohio team.
7. Work to be performed on a fixed price basis.
8. AirWatch and State of Ohio project management will work closely together to ensure that project scope remains consistent and issues are resolved in a timely basis.

Project Costs

- AirWatch will provide the services outlines at a fixed cost of \$9,000.00
 - Services will be billed on the following schedule
 - 50% on acceptance of the SOW
 - 50% on acceptance of all deliverables
- Expenses billed as incurred according to AirWatch travel and expense policy and are the responsibility of State of Ohio for any travel needed outside the Atlanta area.

Service Attachment # 1



AirWatch Maintenance and Support

Effective April 1, 2012

Expires June 30, 2012

Service Attachment # 1

AirWatch Maintenance and Support

	SaaS	On-premise	Appliance
24/7/365 Incident support	•	•	•
Initial incident response times	Severity 1 – 1 hours Severity 2 – 2 hours Severity 3 – 8 hours	Severity 1 – 1 hours Severity 2 – 2 hours Severity 3 – 8 hours	Severity 1 – 1 hours Severity 2 – 2 hours Severity 3 – 8 hours
Self-service portal	•	•	•
Product releases	•	•	•
Upgrade support	Included	Services Purchase	Services Purchase
Cost	Included with Monthly Subscription	20% of License Fees (Annually)	20% of License Fees (Annually)

Effective 01.01.12 | Expires 06.30.12



+1.404.478.7500 | sales@air-watch.com | air-watch.com

Copyright © 2012 AirWatch, Inc. All rights reserved. All other trademarks are the property of their respective owners.

Service Attachment # 1

Terms and Conditions

Annual maintenance and support fees are based on the total software license purchase amount, may be revised pursuant to the EULA, and commences the effective date of the EULA, and are generally billed on an annual basis as provided in the EULA.

The third party appliance hardware is covered by a 1 year limited warranty as defined in the EULA commencing on the delivery date of the third party appliance hardware; annual software maintenance payments after year 1 do not extend such hardware warranty.

An incident is defined as the AirWatch product not working in substantial conformance to the material requirements of the Documentation and/or Specifications. Incidents may be submitted via phone, web, or email.

Severity 1 Defect: A Severity 1 Defect arises when the Software is unable to function properly in a production environment due to a failure of the Software to conform to the Documentation and/or Specifications where such failure has a material adverse impact on the Company's business operations, as a whole. Examples of scenarios that would be considered a Severity 1 Defect include:

- Problems preventing a substantial number of users from getting their emails or using their devices.
- The inability to utilize the console to monitor or manage devices.
- The inability to secure compromised devices through security functions like lock, wipe, and/or partial wipe.

Severity 2 Defect: A Severity 2 Defect arises when the Software is unable to function properly in a production environment due to a failure of the Software to conform to the Documentation and/or Specifications where such failure materially impacts Company's business operations, although the Software remains substantially operational. Examples of scenarios that would be considered a Severity 2 Defect include:

- Problems preventing a significant number of users from getting their emails or using their devices.
- Interruptions of non-critical console functions.

Severity 3 Defect: A Severity 3 Defect arises when the Software is unable to function properly in a production environment due to a failure of the Software to conform to the Documentation and/or Specifications where such failure does not materially impact Company's business operation. Examples of scenarios that would be considered a Severity Level 3 Defect would be issues with reporting or the inability of a few individual users from getting their emails or using their devices.

Effective 04.01.12 | Expires 06.30.12



+1.404.478.7500 | sales@air-watch.com | air-watch.com
Copyright © 2012 AirWatch, LLC. All rights reserved. Proprietary & Confidential.

Service Attachment # 1

Terms and Conditions

Response times are dependent on the Severity levels and are defined as follows:

"Initial Response" means the time it takes from Company's initial web, email or telephone call notification of the Defect until AirWatch responds to the appropriate Company Personnel.

"Interim Resolution" means the time it takes AirWatch to apply a functional resolution to the reported Defect.

"Final Resolution" means AirWatch provides a final correction or modification of the Software that corrects the Defect.

Severity Level	Initial Response	Interim Resolution	Final Resolution
Severity Level 1 Defect	1 hour	6 hours	24 hours
Severity Level 2 Defect	2 hours	12 hours	5 business days
Severity Level 3 Defect	8 hours		Within the next release, or as otherwise agreed upon

Effective 01.01.12 | Expires 06.30.12



+1.404.478.7500 | sales@air-watch.com | air-watch.com
Copyright © 2012 AirWatch, LLC. All rights reserved. Proprietary & Confidential