

## MASTER CLOUD SERVICES AGREEMENT

**THIS MASTER CLOUD SERVICES AGREEMENT ("Agreement")** is by and between AirWatch, LLC ("Service Provider"), having an office at 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338, and the State of Ohio ("State"), through its Department of Administrative Services ("DAS"), having its principal place of business at 30 East Broad Street, 40<sup>th</sup> Floor, Columbus, OH 43215. The State and the Service Provider also are sometimes referred to jointly as the "Parties" or individually as a "Party." The effective date of this Agreement is the date it is signed on behalf of the State ("Effective Date").

### 1. General Information

#### 1.1. Organization

This Agreement covers the licensing of Service Provider's mobile device management software under a SaaS (Software as a Service) model, which includes Service Provider's hosting of its mobile device management software on behalf of the State (the "SaaS Software"), through one or more attachments ("Service Attachments") that describe the SaaS Software that the Service Provider makes available to its customers for license by subscription (the "SaaS License") and that it is authorized to sell to the State. The Service Attachments describe the SaaS Software and the professional services the Service Provider offers under this Agreement, and the End User License Agreement ("EULA") attached hereto as Exhibit A provides the terms or conditions applicable to the SaaS Software, descriptions of professional services, features, and all fees associated with such SaaS Software and professional services, as well as any other provisions to which the Parties have agreed with respect to the SaaS Software. Such EULA and Service Attachments, when executed by the Parties, are incorporated into this Agreement and become a part hereof.

#### 1.2. Subscribing Entities

A "Subscribing Entity" means State agencies, boards, and commissions that place requests through the State's ordering system described in another section ("Orders") under this Agreement for SaaS Licenses identified by one or more Service Attachments to this Agreement. And it includes other entities of the State, such as the legislative and judicial branches of State government and the independent offices of elected State officials that place Orders under this Agreement. It also means the Cooperative Purchasing Members, defined in the next section, that place Orders under this Agreement.

#### 1.3. Cooperative Purchasing Members

"Cooperative Purchasing Members" are entities that qualify for participation in the State's cooperative purchasing program under Section 125.04 of the Ohio Revised Code ("ORC") and that have completed the steps necessary to participate in that program. They may include Ohio political subdivisions, such as counties, townships, municipal corporations, school districts, conservancy districts, township park districts, park districts created under Chapter 1545 of the ORC, regional transit authorities, regional airport authorities, regional water and sewer districts, and port authorities. They also may include any Ohio county board of elections, private fire companies, private, nonprofit emergency medical service organizations, and chartered nonpublic schools.

#### 1.4. Term

The current General Assembly cannot commit a future General Assembly to any expenditure. Therefore, this Agreement along with all Service Attachments will automatically expire at the end of the State's current biennium, which is June 30, 2013.

## MASTER CLOUD SERVICES AGREEMENT

### 1.5. Agreement – Renewal

The State may renew this Agreement in the next biennium by issuing written notice to the Service Provider of the decision to do so. Renewals will be initiated by the State in writing at least 30 days before the expiration of the then current term. This expiration and renewal procedure will also apply to the end of any subsequent biennium.

### 1.6. Service Attachment(s) – Renewal

Along with renewal of this Agreement, the State may renew any or all Service Attachments for the next biennium by issuing written notice to the Service Provider of the decision to do so. Renewals will be initiated by the State at least 30 days before the expiration of the then current term. This expiration and renewal procedure will also apply to any subsequent biennium.

The terms of the renewals for the renewals occurring on the first three anniversaries of the Effective Date of the EULA shall be governed as set forth in the EULA. After the renewals on the first three anniversaries of the Effective Date of the EULA, the Parties agree that the pricing for the SaaS Licenses under any Service Attachment shall be renegotiated by the Parties. Upon termination of this Agreement, all rights of the Subscribing Entities to order additional SaaS Licenses ceases and the Service Provider may not fulfill any such requests for any Subscribing Entity under this Agreement. Further, all existing Service Attachments and all existing Orders under those Service Attachments also will terminate, except to the extent that the Service Provider has any prepaid professional services to perform.

The Subscribing Entities have the option anytime during the Agreement's term to upgrade to a new mobile device management technology or service offering with the Service Provider without incurring any charges for terminating the existing technology or service offering before the agreed upon term of the Subscribing Entity's Order ("Early Termination Charge"), if any such charge is provided for in the applicable Service Attachment. Nothing in the foregoing is meant to imply that upgrades and/or enhancements to a new mobile device management technology or service offering will be without cost to the Subscribing Entities so long as such new mobile device management technology or service offering is offered for a fee to AirWatch's customers.

### 1.7. Relationship of the Parties and Subscribing Entities

The Parties are independent contractors and nothing herein creates or implies an agency relationship, joint venture, or partnership between the Parties. The Service Provider and its officers, employees, contractors, and subcontractors who may attend meetings and work in other situations where their independent contractor status is not obvious to third parties must identify themselves as such to avoid creating an impression that they are State representatives. In addition, neither the Service Provider nor its officers, employees, contractors, or subcontractors may make any representation that they are acting, speaking, representing, or otherwise advocating any position, agreement, service, or otherwise on behalf of the State or any Subscribing Entity.

### 1.8. Audits and Reports

During the term of this Agreement and for three years after its termination, on reasonable notice and during customary business hours, but no more frequently than annually, the State may audit the Service Provider's records and other materials that relate to the SaaS Software and any professional services provided. This audit right also will apply to the State's duly authorized representatives and any organization providing funding for any Order hereunder.

## **MASTER CLOUD SERVICES AGREEMENT**

The Service Provider must make such records and materials available to the State within 15 days after receiving the State's written notice of its intent to audit the Service Provider's records and must notify the State as soon as the records are ready for audit.

If any audit reveals any overcharge to the State in an amount greater than ten percent (10%) of the charge, the State will be entitled to recover the amount of the overcharge and be reimbursed for its reasonable third party costs in connection with the audit. In addition, if any audit reveals any material violation of the terms of this Agreement (other than a material overcharge), the State may terminate this Agreement as provided in the termination section of this Agreement and/or the relevant EULA for cause in accordance with its terms.

The State also may require a reasonable number of various reports from the Service Provider related to the SaaS Software in a mutually agreeable format. Such reports include those identified in Section 7.4 and those identified in any Service Attachment. Further, the State will be entitled to any other reports that the Service Provider makes generally available to its other customers without additional charge. The State's rights under this section will apply to all SaaS Software provided to all Subscribing Entities under this Agreement, but a Subscribing Entity's rights to reports will apply solely to SaaS Licenses it orders or receives under this Agreement.

### **1.9. Subscribing Entities' Reliance on Agreement**

Subscribing Entities may rely on this Agreement. But whenever a Subscribing Entity is a Cooperative Purchasing Member and relies on this Agreement to issue an Order, the Subscribing Entity will step into the shoes of the State under this Agreement for purposes of its Order, and, as to the Subscribing Entity's Order, this Agreement will be between the Service Provider and that Subscribing Entity. The Service Provider must look exclusively to that Subscribing Entity for performance, including but not limited to payment, and must hold the State harmless with regard to such Orders and the Subscribing Entity's performance. But the State, through DAS, will have the right to terminate this Agreement and seek such remedies on termination as this Agreement provides should the Service Provider fail to honor its obligations under an Order from any Subscribing Entity, whether a Cooperative Purchasing Member or not.

### **1.10. Third-Party Suppliers**

The Service Provider must incorporate the costs of any third-party supplies and services in the Service Provider's fees identified on the applicable Service Attachment under this Agreement.

The Service Provider's use of other suppliers does not mean that the State will pay for them. The Service Provider will be solely responsible for payment of its suppliers and any claims of those suppliers for any failure of the Service Provider to meet its obligations under this Agreement in the required manner. The Service Provider will hold the State harmless and indemnify the State against any such claims.

The Service Provider assumes responsibility for all professional services provided under this Agreement whether it or one of its suppliers provides them in whole or in part. Further, the Service Provider will be the sole point of contact with regard to contractual matters, including payment of all charges resulting from the Agreement and all professional service requests.

### **1.11. Non-Exclusivity**

This Agreement is non-exclusive and is not a requirements contract. Nothing herein prevents either Party from entering into similar agreements with other entities.

## **MASTER CLOUD SERVICES AGREEMENT**

### **1.12. Annual Review of Pricing and Services**

For the purposes of maintaining pricing and service competitiveness after the third anniversary of the Effective Date of the EULA, the Service Provider agrees to an annual joint review of its pricing and service offerings. At User's discretion, the annual review may include, discussions based upon AirWatch pricing provided to comparable sized states to the extent that User is able to determine such from publically-available records. Written amendments to the Service Attachments to modify fees and introduce technological improvements to the SaaS Software may be submitted throughout the term of the Agreement.

### **1.13. Conflict Resolution**

If a Party is noncompliant with any term or condition of this Agreement or if a dispute arises under this Agreement, the Party raising the dispute may provide to the other Party written notice referencing this section and specifying the nature of the dispute (the "Dispute Notification"). The Parties then will seek to resolve the dispute in accordance with the procedures in this Section.

All disputes will be submitted first to the State's Contract Manager and the Service Provider's Account Manager (or equivalent) for resolution. For 15 days from the date of receipt of the Dispute Notification ("Dispute Date"), the State Contract Manager and Service Provider's Account Manager will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If after the 15 days identified above, the State's Contract Manager and the Service Provider's Account Manager are unable to resolve the dispute, the Parties will then submit the dispute to the Network Administrator and to the Service Provider's Sales Manager (or equivalent) for resolution. For the next 15 days, the Network Administrator and Service Provider's Sales Manager will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If after the 15 days identified above, the State's Network Administrator and the Service Provider's Account Manager are unable to resolve the dispute, the Parties will then submit the dispute to the State Chief Operating Officer and to the Service Provider's Sales Director (or equivalent) for resolution. For the next 15 days, the Chief Operation Officer and Service Provider's Sales Director will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If following the 15 days in the previous section, the Chief Operating Officer and the Service Provider's Sales Director are unable to resolve the dispute, the Parties will then submit the dispute to the State's Chief Information Officer and to the Service Provider's Vice President of Sales (or equivalent executive) for resolution. For the next 15 days, the State's Chief Information Officer and Service Provider's Vice President will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith. If the State's Chief Information Officer and Service Provider's Vice President are unable to resolve the dispute within that time, the Parties will nevertheless continue to retain their rights to initiate formal proceedings hereunder.

The specific format for such discussions will be left to the discretion of the representatives of the State and Service Provider responsible for attempting to resolve the dispute, but each Party will involve the business and legal resources reasonably necessary to attempt in good faith to resolve the dispute at the earliest possible time and without undue delay.

If the Parties are unable to resolve the dispute and the dispute involves a claim that the Service Provider is noncompliant with its obligations hereunder or has overcharged for the SaaS Licenses or a service, the State or affected Subscribing Entities may withhold payment for any items that are the subject of the dispute until the Service Provider cures

## **MASTER CLOUD SERVICES AGREEMENT**

the noncompliance, the Parties arrive at an agreement to resolve the dispute, or a Party obtains a resolution in a court of competent jurisdiction.

Nothing in this Section is intended to limit the rights provided under Section 6 or be a prerequisite to exercising those rights.

Once the dispute has been resolved, any payments withheld will be handled in the following manner:

If the resolution was in favor of the State or one or more Subscribing Entities, the Service Provider will issue a credit on the next invoice for the affected Subscribing Entities. If the credit exceeds the SaaS Software charges on the next invoice or an invoice will not be issued within 60 days of the resolution, the Service Provider will issue payment in the form of a check in the amount exceeding the Service charges or for the full amount if an invoice will not be issued within 60 days. Any such checks must be issued within that 60-day period.

If in favor of the Service Provider, the affected Subscribing Entities will submit appropriate payment within 30 days of receiving notification of the resolution at the office designated to receive the invoice.

In either of the above cases, the amount or amounts withheld by the State or Subscribing Entity(s) will be taken into account in calculating any amount(s) due.

## **2. General Requirements for Cloud Services**

### **2.1. Standards**

All SaaS Software shall perform as defined in the EULA and in the Documentation (as that term is defined in the EULA). Service Provider provides and maintains a redundant infrastructure that will ensure access for all of the State's enrolled users to the SaaS Software in the event of failure at any one of the Service Provider locations, with effective contingency planning (including back-up and disaster recovery capabilities), and, under its maintenance and support program, maintains a 24/7/365 trouble shooting service for inquiries, outages, issue resolutions, etc. The maintenance and support program provided by the Service Provider shall be as described in the EULA. The Service Provider has and will continue to use its best efforts through quality assurance procedures to ensure that there are no viruses or malware or undocumented features in its infrastructure and the SaaS Software and that they do not contain any embedded device or code (e.g., time bomb) that is intended to obstruct or prevent any use of or access to them by the Subscribing Entities.

User access to the SaaS Software must be capable of being integrated with a Subscribing Entity's Active Directory (or other LDAP service) to support single sign-on capability for users and to ensure that every user is tied to an Active Directory or other LDAP account and to prevent user access when a user is disabled or deleted in the applicable Subscribing Entity's Active Directory or other LDAP service.

Audits of the Service Provider's operations will be regularly conducted at the sole expense of the Service Provider and a copy of such audits must be provided to the State within 30 days of its completion each year.

At no cost to the State, the Service Provider must promptly remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the SaaS Software within a commercially reasonable time.

### **2.2. Object Reassignment**

The Service Provider licenses the SaaS Software on a per Device basis and (i) the SaaS Software may only be used or accessed by the State or Subscribing Entities on no more

## **MASTER CLOUD SERVICES AGREEMENT**

than the number of Devices specified on each Service Attachment, but the SaaS License may be transferred from Device to Device without additional charge and (ii) there is no limit on the number of computers from which the Devices may be monitored using the SaaS Software. A later section in this Agreement governs assignment of a Subscribing Entity's subscription to any Service to a successor in interest.

### **2.3. Generated Files**

"Generated Files" are files storing information, instructions, or data that the State creates or modifies using the Service Provider's SaaS Software and in which the data or other information was provided or created by a Subscribing Entity. Such Generated Files are also included in the definition of "State Data" in a later section of this Agreement. Examples of such files could include, among others, text files generated with a word processor, data tables created with a database engine, and image files created with a graphics application. Any of the Service Provider's proprietary information that would allow the State or a third party to enumerate how the SaaS Software functions is not included in the term "Generated Files." As between the State and the Service Provider, the State will own all Generated Files that the State prepares by using the Services, excluding such portions of the Generated Files that consist of embedded portions of the Software. The Service Provider or its licensors will retain ownership of any portions of the Software embedded into Generated Files. But the Service Provider grants to the State a nonexclusive, royalty-free right to reproduce and distribute to third parties any portions of the intellectual property embedded in any Generated Files that the State creates while using the Services in the manner in which the Services are designed to be used. In the State's distribution of the Generated Files, the State may not use the Service Provider's name, logo, or trademarks, except to the extent that such are incorporated in such Generated Files by the design of the SaaS Software when used as intended.

### **2.4. Service Provider Warranties**

The Service Provider warrants that it has validly entered into this Agreement and has the legal power to do so. For any breach of a warranty above, State's and individual Subscribing Entities' remedies will be as provided in the section of this Agreement dealing with termination. Other warranties and remedies related specifically to the SaaS Software are set forth in the EULA.

### **2.5. State Responsibilities**

The State will (i) be responsible for its compliance with this Agreement and the EULA and (ii) be responsible for the accuracy, quality, and legality of its data and of the means by which it acquired that data. The State may not (a) use the SaaS Software to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (b) intentionally use the SaaS Software to store or transmit Malicious Code, (c) intentionally interfere with or disrupt the integrity or performance of the SaaS Software or third-party data contained therein, (d) attempt to gain unauthorized access to the SaaS Software or its related systems or networks, or (e) violate any of the use restrictions set forth in the EULA. In the event that any third party proposed to provide management, staging, support, hosting, or similar services with regard to the SaaS Software on its behalf is a Service Provider Competitor, the Service Provider's prior written consent shall be required, which consent shall not be unreasonably withheld. For purposes hereof, "Service Provider Competitor" means any entity that provides any software, product, or service that is competitive with the SaaS Software such as those companies considered by Gartner, Inc. in creating its "MDM Magic Quadrant," including, without limitation, those companies considered industry

## MASTER CLOUD SERVICES AGREEMENT

leaders or industry visionaries such as Sybase, Good Technology, MobileIron, Zenprise, Symantec, and McAfee, but excludes major outsourcers such as IBM and CGI.

### 3. Insurance, Indemnification, Limitation of Liability

#### 3.1. Insurance

The Service Provider must provide the following insurance coverage at its own expense throughout the term of this Agreement to the State:

- (A) Workers' compensation insurance, as required by Ohio law, and if some work will be done outside Ohio, the laws of the appropriate states where work will be done. The Service Provider also must maintain employer's liability insurance with at least a \$1,000,000.00 limit.
- (B) Commercial General Liability insurance coverage for bodily injury, personal injury, wrongful death, and property damage. The defense cost must be outside of the policy limits. Such policy must designate the State of Ohio as an additional insured, as its interest may appear. The policy also must be endorsed to include a blanket waiver of subrogation. At a minimum, the limits of the insurance must be:

- \$ 2,000,000 General Aggregate
- \$ 2,000,000 Products/Completed Operations Aggregate
- \$ 1,000,000 per Occurrence Limit
- \$ 1,000,000 Personal and Advertising Injury Limit
- \$ 100,000 Fire Legal Liability
- \$ 10,000 Medical Payments

The policy must be endorsed to provide the State with 30-days prior written notice of cancellation or material change to the policy. And the Service Provider's Commercial General Liability must be primary over any other insurance coverage.

- (C) Commercial Automobile Liability insurance with a combined single limit of \$500,000.
- (D) Professional Liability insurance covering all staff with a minimum limit of \$1,000,000 per incident and \$3,000,000 aggregate. If the Service Provider's policy is written on a "claims made" basis, the Service Provider must provide the State with proof of continuous coverage at the time the policy is renewed. If for any reason the policy expires, or coverage is terminated, the Service Provider must purchase and maintain "tail" coverage through the applicable statute of limitations.

All certificates must be in a form that is reasonably satisfactory to the State as to the contents of the policies and the quality of the insurance carriers and must identify this Agreement. All carriers must have at least an "A-" rating by A.M. Best.

Any Subscribing Entity that is a Cooperative Purchasing Member that orders SaaS Licenses also may require a certificate of insurance from the Subscribing Entity naming it as an additional insured for the duration of such work on the Subscribing Entity's premises.

#### 3.2. Indemnification for Bodily Injury and Property Damage

The Service Provider must indemnify the State and the Subscribing Entities against all liability or expense resulting from bodily injury to any person (including death) or damage to property arising out of its performance under this Agreement, provided such bodily

## **MASTER CLOUD SERVICES AGREEMENT**

injury or property damage is due to the negligence or other tortious conduct of the Service Provider, its employees, agents, or subcontractors.

### **3.3. Indemnification for Infringement**

The Service Provider will provide indemnification for infringement as provided in the EULA.

### **3.4. Limitation of Liability**

NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES, OR ANY LOST PROFITS, OR REVENUE. EXCEPT FOR PERSONAL INJURY (INCLUDING DEATH), PROPERTY DAMAGE, OR INTELLECTUAL PROPERTY INFRINGEMENT CLAIMS, EITHER PARTY'S MAXIMUM LIABILITY FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE EULA, ANY QUOTE, OR ANY ORDER PLACED USING TSR, WHETHER SUCH ACTION IS BROUGHT IN LAW, EQUITY, CONTRACT, OR TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE, SHALL BE LIMITED TO THE USER LICENSE FEES PAID BY USER IN THE LAST TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, LESS ALL PAYMENTS MADE IN RESPECT OF OTHER CLAIMS SUBJECT TO THIS LIMITATION. WITH RESPECT TO BREACHES OF SECTIONS 3 OR 9 OF THE EULA, (A) THE BREACHING PARTY SHALL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES, OR ANY LOST PROFITS, OR REVENUE, PROVIDED HOWEVER THAT EITHER PARTY'S MAXIMUM LIABILITY FOR ANY DAMAGES RELATED TO SUCH BREACHES, WHETHER SUCH ACTION IS BROUGHT IN LAW, EQUITY, CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE, SHALL BE LIMITED TO THE USER LICENSE FEES PAID BY USER IN THE LAST TWENTY-FOUR (24) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, LESS ALL PAYMENTS MADE IN RESPECT OF OTHER CLAIMS SUBJECT TO THIS LIMITATION UNDER THIS EULA.

## **4. Confidentiality, Proprietary Rights, and Handling of Data**

### **4.1. Confidentiality**

Either Party (the "Disclosing Party") may disclose to the other Party (the "Receiving Party") written material or oral or other information that the State treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the Disclosing Party delivers to the Receiving Party will remain with the Disclosing Party. The Receiving Party must treat such Confidential Information as secret if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interests of the public, other contractors or potential contractors with the Disclosing Party, or individuals or organizations about whom the Disclosing Party keeps information. The Receiving Party may not disclose any Confidential Information to third parties and must use it solely to perform under this Agreement.

If any item delivered under this Agreement contains data, documentation, or other written information that is confidential in nature and properly labeled as such, then it also will be Confidential Information for purposes of this section. The Receiving Party will keep all such Confidential Information in confidence and will not use it other than as authorized under this Agreement. The Receiving Party shall not disclose any such Confidential Information to any third party (i) except on a need to know basis and (ii) without first obligating the third party to maintain the secrecy of the Confidential Information.

## MASTER CLOUD SERVICES AGREEMENT

If the Disclosing Party discloses Confidential Information to the Receiving Party, the Receiving Party's obligation to maintain the confidentiality of the Confidential Information will not apply where such:

- (1) Was already in the possession of the Receiving Party without an obligation of confidence;
- (2) Is independently developed by the Receiving Party, provided documentary evidence exists to support the independent development;
- (3) Except as provided in the next paragraph, is or becomes publicly available without a breach of this Agreement;
- (4) Is rightfully received by the Receiving Party from a third party without an obligation of confidence;
- (5) Is disclosed by the Receiving Party with the written consent of the Disclosing Party; or
- (6) Is released under a valid order of a court or governmental agency, provided that the Receiving Party:
  - (a) Notifies the Disclosing Party of the order immediately upon receipt of it, unless it is legally prohibited from doing so; and
  - (b) Makes a reasonable effort to obtain a protective order from the issuing court or agency limiting the disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things, is nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Agreement. Therefore, if the Receiving Party is provided with access to such information, item (3) in the preceding paragraph does not apply, and the Receiving Party must treat such information as Confidential Information whether it is available elsewhere or not.

The Receiving Party must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Agreement.

The disclosure of the Confidential Information of the Disclosing Party in a manner inconsistent with the terms of this provision may cause the Disclosing Party irreparable damage for which remedies other than injunctive relief may be inadequate, and each Receiving Party agrees that in the event of a breach of the Receiving Party's obligations hereunder, the Disclosing Party will be entitled to temporary and permanent injunctive relief to enforce the provisions of this Agreement without the necessity of proving actual damages. However, this provision does not diminish or alter any right to claim and recover damages.

#### 4.2. Public Records Requests.

Should the Service Provider receive any public records request with respect to any State Data, the Service Provider will immediately notify the affected Subscribing Entity or Entities and fully cooperate with the affected Subscribing Entity or Entities as it or they direct, so long as such directions are lawful.

#### 4.3. Handling of the State's Data

As part of its operation, the SaaS Software (i) does not collect, use, or access information about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar; (ii) does not access information passing through the Device, such as texts, emails, text files, data tables, or image files; (iii) and does not access information stored on a Device. In managing Devices, the SaaS

## **MASTER CLOUD SERVICES AGREEMENT**

Software only accesses uses information necessary to identify individual Devices and Device profiles and the information necessary to manage devices such as the names of the applications installed on the Device and the operating system for a Device. "State Data" is any information, data, files, or software that the State or its Subscribing Entities use or store on or in conjunction with the SaaS Software, including but not limited to Generated Files. As a part of the normal operation of the SaaS Software, the Service Provider would have no access to State Data, the Service Provider would not store State Data, and the Parties do not contemplate that the Service Provider will be provided access to State Data. The Service Provider employs industry-standard physical, logical, and electronic security and confidentiality systems to protect the confidentiality of information. If the State requires the Service Provider to access the State Data, the Service Provider shall provide a quote to the State for any costs associated with enhanced security procedures beyond industry-standard physical, logical, and electronic security and confidentiality systems.

Should the Service Provider be provided with access the State Data, the Service Provider must use due diligence to ensure computer and telecommunications systems and software involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. To accomplish this, the Service Provider must comply with all applicable National Institute of Standards and Technology ("NIST") standards for Moderate Impact systems and:

- (1) Apply appropriate risk management techniques to ensure security for all sensitive data, including but not limited to any data identified as Confidential Information elsewhere in this Agreement.
- (2) Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
- (3) Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as and detect and respond to those threats and vulnerabilities.
- (4) Maintain appropriate identification and authentication process for information systems and software associated with State Data.
- (5) Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- (6) Implement and manage security audit logging on information systems, including computers and network devices.

The Service Provider must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disabling all others. To do this, the Service Provider must use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available. The Service Provider must use two-factor authentication to limit access to systems that contain State Data.

Unless the State, through the applicable Subscribing Entity, instructs the Service Provider otherwise in writing, the Service Provider must assume all State Data is both confidential and critical for State operations, and the Service Provider's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity. As part of the Service

## **MASTER CLOUD SERVICES AGREEMENT**

Provider's protection and control of access to and use of data, the Service Provider must employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Service Provider's infrastructure associated with State Data. Further, the Service Provider must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with State Data.

The Service Provider must use appropriate measures to ensure that State's data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the data must be appropriate to the situation and may include erasure, destruction, or encryption of the data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Service Provider's obligations under this Agreement.

The Service Provider must have a business continuity plan in place. The Service Provider must test and update the IT disaster recovery portion of its business continuity plan at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Service Provider maintains State Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with State Data in the case of a disaster or other business interruption. The Service Provider's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to State Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Service Provider also must provide for reviewing, testing, and adjusting the plan on an annual basis.

The Service Provider may not allow State Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Agreement properly. Even then, the Service Provider may permit such only if adequate security measures are in place to ensure the integrity and security of the data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas. At a minimum, portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network. The Service Provider also must maintain an accurate inventory of all such devices and the individuals to whom they are assigned. The Service Provider's backups remain at its data centers, with the primary data center's data is backed up to the backup data center and vice versa. The Service Provider stores such data in its data centers in an unencrypted format, but encrypts the data whenever it is in transit.

Any encryption requirement identified in this provision must meet the NIST standards identified above.

The Service Provider must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Service Provider also must maintain an incident response capability for all security breaches involving State Data whether involving mobile devices or media or not. The Service Provider must detail this capability in a written policy that defines procedures for how the Service Provider will

## MASTER CLOUD SERVICES AGREEMENT

detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State Data or the infrastructure associated with State Data.

In case of an actual security breach that may have compromised State Data, including but not limited to loss or theft of devices or media, the Service Provider must notify the State in writing of the breach within 24 hours of the Service Provider becoming aware of the breach, and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State Data that is inconsistent with the terms of this Agreement and of which the Service Provider becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Agreement by an employee, agent, or subcontractor of the Service Provider.

The Service Provider must give the State full access to the details of the breach, must document all such incidents, including its response to them, and make that documentation available to the State on request.

All State Data will remain the property of the State. The Service Provider must ensure that the State retains access and download capability for purposes of retrieving its data for research, investigation, transfer, or migration to other systems, it being understood that the State may not have access to and retain the Service Provider's proprietary information that would allow the State or a third party to enumerate how the SaaS Software functions.

All State Data at rest in systems supporting the Service Provider's SaaS Software must reside within the contiguous United States with a minimum of two data center facilities at two different and distant geographic locations and be handled in accordance with the requirements of this section at all Service Provider locations. Currently, Savvis Communications Company's Norcross, GA facility serving as the Service Provider's primary data center; AT&T Hosting & Application Services' Dallas TX facility serving as the Service Provider's secondary data center; and Level 3 Communications, LLC's Atlanta, GA facility serving as the Service Provider's tertiary data center.

#### 4.4. Return of State Data

At no additional cost to the Subscribing Entity, upon request made no more frequently than quarterly during a SaaS License term or once within 90 days after the effective date of termination or expiration of the Subscribing Entity's Order for that Service, the Service Provider will make available to the Subscribing Entity for download the State Data, if any, covered by that terminated or expired SaaS License, as well as any Generated Files, in native format or any other format the Subscribing Entity reasonably requests within five (5) business days of the request and at no additional charge to the Subscribing Entity. After such 90-day period, the Service Provider will have no obligation to maintain the State Data covered by an expired Service Order and must thereafter, unless legally prohibited, delete the applicable State Data in its systems or otherwise in its possession or under its control.

#### 4.5. Proprietary Rights

Subject to the limited rights expressly granted hereunder and under the EULA, the Service Provider reserves all rights, title, and interest in and to the SaaS Software, including all related intellectual property rights. No rights are granted to the State or Subscribing Entities hereunder other than as expressly set forth herein or elsewhere in the Agreement.

Subscribing Entities will not intentionally permit any third party to access the SaaS Software, except as permitted herein or in an Order Form, create derivative works based on the SaaS Software except as permitted herein or elsewhere in the Agreement, reverse engineer the SaaS Software, or access the SaaS Software to build a competitive product

## MASTER CLOUD SERVICES AGREEMENT

or service or to copy any features, functions, or graphics of the SaaS Software. Nothing herein prohibits a Subscribing Entity from porting and hosting Generated Code, as defined in this Agreement, to other sites to support its own internal business purposes during and after any term of an Order.

If a Subscribing Entity, a third party acting on a Subscribing Entity's behalf, or a user creates applications or program code to facilitate use of the SaaS Software without violating the license restrictions set forth in the EULA, the Subscribing Entity authorizes the Service Provider to host, copy, transmit, display, and adapt such applications and program code, solely as necessary for the Service Provider to provide the mobile device management with the SaaS Software in accordance with this Agreement. Subject to the above, the Service Provider acquires no right, title or interest from the Subscribing Entity or its licensors under this Agreement in or to such applications or program code, including any intellectual property rights therein, and the Subscribing Entity is entitled to port, use, and host such anywhere.

Subject to the limited rights granted by the State hereunder, the Service Provider acquires no right, title, or interest from the State or its licensors under this Agreement in or to the State Data, including any intellectual property rights therein.

### 4.6. Disentanglement Services

On termination, in whole or in part, or expiration of an Order for any reason, the Service Provider will perform disentanglement services if requested by Subscribing Entity to transition responsibility for the provision of mobile device management services to another service provider or to Subscribing Entity itself ("Disentanglement Services"). Such Disentanglement Services will be provided at the rates specified in the applicable Service Attachment. In connection with Disentanglement Services, the State and all Subscribing Entities must have Service Provider's prior written consent to engage any Service Provider Competitor who will (i) operate, use, or view the SaaS Software or Documentation, (ii) engage in competitive analysis, benchmarking, or evaluation, of the SaaS Software or Documentation, or (iii) create any derivatives based upon the SaaS Software or Documentation, whether for the use of User or the use of Service Provider Competitor. Nothing herein shall prevent User from engaging a succeeding supplier to mobile device management services who is a Service Provider Competitor and, at the request of User, such succeeding supplier may receive database information from Service Provider.

On request, the Service Provider will immediately provide a quote for such Disentanglement Services based on the rate(s) in the applicable Service Attachment and on issuance of an Order for the Disentanglement Services, the Service Provider will immediately begin providing necessary and appropriate assistance to allow mobile device management services to continue without interruption and to facilitate the transfer of mobile device management services to the ordering Subscribing Entity or its designee.

The Service Provider will provide the Disentanglement Services so that minimize risk and maximize predictability are afforded to the Subscribing Entity. This includes at a minimum all efforts necessary for knowledge transfer to the succeeding supplier (or to the Subscribing Entity's internal resources), upon the Subscribing Entity's request and issuance of an Order for the Disentanglement Services. As a part of the Disentanglement Services, the Subscribing Entity shall not be entitled to receive or transfer any of the Service Provider's proprietary information that would allow the State or a third party to enumerate how the SaaS Software functions. As used herein "knowledge transfer" shall not include any of the Service Provider's proprietary information.

## MASTER CLOUD SERVICES AGREEMENT

At the expense of the Subscribing Entity, the Service Provider will assist the Subscribing Entity in developing a plan that will specify the tasks to be performed by the parties during disentanglement and the schedule for the performance of such tasks. The plan will be developed, implemented, and concluded with full disentanglement with all due speed, not to exceed 90 days.

At the expense of the Subscribing Entity, the Service Provider will participate in all disentanglement meetings as reasonably requested by the Subscribing Entity.

At the Subscribing Entity's request, the Service Provider will return all data as further stipulated in the previous section.

At the expense of the Subscribing Entity, the Service Provider will take part in parallel operations and continue to perform the mobile device management alongside resources supplied by the succeeding service provider or, as the case may be, the Subscribing Entity.

Additionally, at the expense of the Subscribing Entity, the Service Provider will provide knowledge transfer for all incoming personnel who will assume responsibility for mobile device management after termination or expiration of this Agreement, and the Service Provider will cooperate with all third parties in the Subscribing Entity IT Environment during disentanglement.

At the expense of the Subscribing Entity, the Service Provider's personnel appropriate for knowledge transfer will be dedicated to the Subscribing Entity for the duration of the disentanglement and thereafter for up to 12 months, if the Subscribing Entity requests.

The Service Provider will turn over any tools, software, equipment, tools, and any other materials owned by the Subscribing Entity, if any.

All Disentanglement Services will be performed as expediently and efficiently as reasonably possible to facilitate a timely, cost effective, and organized disentanglement.

If necessary to complete the disentanglement and requested in writing by the Subscribing Entity, for a period no longer than three (3) months, the Service Provider will continue to provide the SaaS Software for which the applicable Order has expired or terminated on a month to month basis in exchange for a monthly fee equal to the monthly cost to the Subscribing Entity of the SaaS Software under the applicable expired or terminated Order.

### 4.7. State Responsibilities

The State will be responsible for its compliance with this Agreement, be responsible for the accuracy, quality, and legality of State Data and of the means by which it acquired State Data, use commercially reasonable efforts to prevent unauthorized access to or use of the SaaS Software, and notify the Service Provider promptly of any unauthorized access or use of which it becomes aware. Further, the State will use the SaaS Software only in accordance with the terms and conditions set forth in the Agreement, EULA and the Documentation (as such term is defined in the EULA), to the extent not inconsistent with the State's rights under applicable laws and government regulations.

Further, the State may not intentionally make the SaaS Software available to anyone other than its employees and its contract personnel who are not Service Provider Competitors, sell, resell, rent, or lease the SaaS Software, use the SaaS Software to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights. The State also may not intentionally use the SaaS Software to store or transmit Malicious Code, intentionally

## **MASTER CLOUD SERVICES AGREEMENT**

interfere with or disrupt the integrity or performance of the SaaS Software or third-party data contained therein, or attempt to gain unauthorized access to the SaaS Software or their related systems or networks.

### **5. Orders, Requesting Service, Delivery, Acceptance, Termination, and Modification**

#### **5.1. Acceptance**

The acceptance procedure for set up or installation of the SaaS Software will be a review by the Subscribing Entity acquiring the SaaS Software to ensure that it meets the performance standards and other requirements in the applicable Service Attachment and, if ordering documents ("Order Forms") are authorized in the applicable Service Attachment, the applicable Order Form and that the installation has been done in a professional manner. For professional services, the acceptance procedure will be a review by the Subscribing Entity to ensure the professional service complies with the performance requirements in the applicable Service Attachment. The Subscribing Entity will have up to 15 days after the installation or the establishment of the SaaS Software or the completion of the performance of professional services to do this. The Subscribing Entity will not issue a formal letter of acceptance, unless otherwise specified in the applicable Service Attachment, and passage of 15 days will imply acceptance, though the Subscribing Entity will issue a notice of noncompliance if set up or installation or professional services do not meet the requirements in this Agreement.

If the Subscribing Entity issues a noncompliance letter, the Service Provider will have 30 days to correct the problems listed in the letter. If the Subscribing Entity has issued a noncompliance letter, the SaaS Software, installation, or set up will not be accepted until that Subscribing Entity issues a letter of acceptance indicating that each problem noted in the noncompliance letter has been cured. If the problems have been fixed during the 30-day period, the Subscribing Entity will issue the acceptance letter within 15 days after all defects have been fixed. Passage of 15 days will imply acceptance. If the Service Provider fails to correct the defect(s), the applicable Order(s) will terminate without cost or obligation to the Subscribing Entity.

#### **5.2. Service, Termination, or Modification**

All Orders for SaaS Software, as well as any termination of an Order or modification to an Order, must be made through the State's Technology (formerly Telecommunications) Service Request ("TSR") system or any replacement system used by the State at the time an Order for SaaS Software, termination, or modification is requested. Therefore, the Service Provider must notify the State when an Order is received that was placed outside the TSR, or a replacement system, and the Service Provider will not accept the Order. If a Service Provider accepts an Order outside the TSR, or any replacement system, the State or the Subscribing Entity may either withhold payment for the unverified Order and require termination of the Service under the unverified Order without penalty to the State or the Subscribing Entity or accept the unverified Order.

The Service Provider agrees to keep Subscribing Entities' Orders updated and current in the TSR System.

The Service Provider is responsible for processing all Orders, billing, payments, cancellations, changes, and receiving and managing all service calls in a consolidated manner. In this regard, the Service Provider must act as the sole point of contact for the SaaS Software and professional services under this Agreement, the EULA, and any related Service Attachments for all Subscribing Entities. The Service Provider may not require a Subscribing Entity to contact any of the Service Provider's third-party suppliers

## MASTER CLOUD SERVICES AGREEMENT

or otherwise transact business directly with such suppliers for any SaaS Licenses ordered under this Agreement, and in all respects, the Service Provider must maintain a seamless, single-point-of-contact business relationship with each Subscribing Entity for the SaaS Licenses ordered under this Agreement.

### 6. Termination – Agreement, Service Attachments, Orders

#### 6.1. Termination by the State

The Service Provider must comply with all terms and conditions of this Agreement. If the Service Provider fails to perform any one of its obligations under this Agreement, it will be in default, and the State may proceed in any or all of the following ways:

1. The State may terminate this Agreement, the applicable Service Attachment(s), or the affected Order(s) under this Agreement;
2. The State may withhold payment for any affected SaaS Licenses until the Service Provider cures the noncompliance or the Parties arrive at an agreement as to the corrective action for the noncompliance; or
3. The State may file a complaint for damages with a court of competent jurisdiction in Ohio.

The State also may terminate this Agreement or any Service Attachments for its convenience with 30 days written notice to the Service Provider. In any such event, each Subscribing Entity must pay for all accrued and unpaid charges for the SaaS Licenses and any professional services, through the effective date of such termination.

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails at any time to continue funding for the payments and other obligations due as part of this Agreement, the State's obligations under this Agreement will terminate as of the date the funding expires without further obligation of the State.

#### 6.2. Termination of Orders by Subscribing Entity or Service Provider

Under this Agreement, specific Orders also may be terminated by either a Subscribing Entity or the Service Provider, as follows:

##### 6.2.1. By a Subscribing Entity

A Subscribing Entity may terminate the SaaS Licenses under any Order it has placed, and it may do so at any time for any or no reason. The Subscribing Entity will be liable for charges accrued but unpaid as of the termination date, as well as any Early Termination Charge outlined in the appropriate Service Attachments.

If the Subscribing Entity's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly or other governmental body, and the General Assembly or other governmental body fails at any time to continue funding for the payments and other obligations due under an Order, the Subscribing Entity's obligations with respect to that Order will be terminated as of the date the funding expires, and the Subscribing Entity will have no further obligation with respect to such Order, including but not limited to any Early Termination Charge outlined in any affected Service Attachments.

If a termination of any SaaS License under one or more Orders is for cause or non-appropriation of funds, as described in Section 6, the Subscribing Entity will not be liable for any Early Termination Charge, if such are otherwise applicable to the SaaS License or SaaS Licenses so terminated.

## **MASTER CLOUD SERVICES AGREEMENT**

### **6.2.2. By the Service Provider**

If a Subscribing Entity materially defaults in the performance of any of its duties or obligations under this Agreement, the Service Provider, by giving at least 30 days prior written notice, may cancel any affected SaaS Licenses provided to that Subscribing Entity under this Agreement.

If the Subscribing Entity cures the default to the satisfaction of the Service Provider and before the date of cancellation for any affected SaaS Licenses, the Order will remain in full force and effect.

The Subscribing Entity will remain liable for charges accrued but unpaid as of the cancellation date and any Early Termination Charge as outlined in the appropriate Service Attachment(s).

## **7. Financial – Fees, Claims and Disputes, Billing, and Payment**

### **7.1. Fees**

All applicable charges are fully documented in the appropriate Service Attachment(s). The Subscribing Entity will not be responsible for any charges not documented in the applicable Service Attachment(s) nor will the Subscribing Entity be responsible for any charges waived by the Service Provider in this Agreement or the applicable Service Attachment(s).

Subscribing Entities are not subject to increases in fees during the term of this Agreement.

Subscribing Entities are not responsible for any charges from the Service Provider's third-party suppliers for any SaaS Licenses ordered under this Agreement, unless an applicable Service Attachment expressly provides otherwise. In this regard, the Service Provider is the seller or reseller of the Service Provider's third-party suppliers, and any payments due to the Service Provider's third-party suppliers under this Agreement are included in the Service Provider's fees specified in the applicable Service Attachment, unless that Service Attachment expressly provides otherwise.

### **7.2. Billing**

Invoices will be issued at the Order level, but the Subscribing Entity may require a recap at the agency, division, or district level based on the organizational structure of the Subscribing Entity.

Invoices must be submitted to the office designated in the purchase order or TSR as the "bill to address." The invoice must be submitted within 60 days of the end of each month in which SaaS Licenses are in use by Subscribing Entities or, in the case of professional services, within 60 days of the end of each month in which professional services are provided. If the Subscribing Entity does not receive the invoice within the 60 days of the dates described herein, the Subscribing Entity will be entitled to deny payment of the invoice.

A proper invoice must include the following information and/or attached documentation:

1. Name and address of the Service Provider as designated in this Agreement;
2. Federal Tax Identification Number of the Service Provider as designated in this Agreement;
3. Invoice remittance address as designated in the Agreement; and
4. A sufficient description of the SaaS Licenses and professional services, if any, to allow the Subscribing Entity to identify them and perform an audit.

## MASTER CLOUD SERVICES AGREEMENT

### 7.3. Payment

Payments for SaaS Licenses and professional services under this Agreement will be due on the 30th calendar day after the actual receipt of a proper invoice in the office designated to receive the invoice.

The Service Provider agrees to receive payment from approved vouchers by electronic fund transfer ("EFT") for Subscribing Entities that rely on them to make payment. The Service Provider will cooperate with Subscribing Entities in providing the necessary information to implement EFT. The date the EFT is issued in payment will be considered the date payment is made, or if a Subscribing Entity does not use an EFT process, the date its check or warrant is issued in payment will be considered the date payment is made.

### 7.4. State Reporting Requirements

The Service Provider must provide the State with a recap of all SaaS License fees charged to the Subscribing Entities on a monthly basis and all professional services provided to the Subscribing Entities on a monthly basis. Additional, specific reporting data requirements may be outlined in the Service Attachment(s).

### 7.5. Service Level Guarantee and Credits

Section 10.4 of the attached EULA provides all Service Level Agreements and remedies.

### 7.6. Cost Recovery OK. We need to provide titles.

The Service Provider must pay a Cost Recovery Fee to the State to cover the estimated costs the State will incur administering this Agreement and the SaaS Licenses and professional services offered under it.

The Cost Recovery Fee will be 2% of the total dollar amount of SaaS Licenses and professional services the Service Provider invoices under this Agreement to all Subscribing Entities, including all Cooperative Purchasing Members. The State will generate notification to the Service Provider via email on the last day of the calendar quarter advising the Service Provider to complete a revenue reporting form provided by the State within 30 days after the close of the quarter. The State may compare the form provided by the Service Provider to information in the State's accounting system, the TSR, and other records for purposes of verifying the accuracy of the form. The Parties will meet to resolve any accounting discrepancies. If the discrepancies cannot be resolved, the State may generate an invoice to the Service Provider for the quarterly Cost Recovery Fee based on reported revenue from the Service Provider or the State's records, whichever is greater. Any unresolved discrepancies shall be subject to the dispute resolution provisions of this Agreement.

Example of calculation of a Cost Recovery Fee:

#### Example 1

Service Provider Revenue Report	\$1,000.00	X 2%	\$20.00
State Expenditure Report	\$900.00		

#### Example 2

Service Provider Revenue Report	\$800.00		
State Expenditure Report	\$1,000.00	X 2%	\$20.00

## MASTER CLOUD SERVICES AGREEMENT

The Service Provider must remit to the State the 2% Cost Recovery Fee within 30 days of receipt of the invoice from the State by check to the State of Ohio, Office of Information Technology. The check must be made payable to the Treasurer, State of Ohio, Fund 133, and must be sent to the State at the following address:

Department of Administrative Services  
Office of Information Technology  
Infrastructure Services Division  
30 E. Broad Street – 39<sup>th</sup> Floor  
Columbus, OH 43215  
Attn: Business Manager

To ensure that the payment is credited properly, the Service Provider must identify the check as a State of Ohio Cost Recovery Fee and reference this Agreement and the Quarterly Activity Reports supporting the check amount. The data requirements for the Quarterly Activity Reports will be detailed in the Service Attachment(s). Credit of the Cost Recovery Fee will begin in the month of execution of this Agreement.

A copy of the Quarterly Activity Report will be sent to the Contract Manager at the following address:

Department of Administrative Services  
Office of Information Technology  
Infrastructure Services Division  
1320 Arthur E. Adams Drive, 3rd Floor  
Columbus, Ohio 43221  
Attention: Contract Manager

The first payment will be calculated against all SaaS License fees and professional services fees rendered to the existing Subscribing Entities transferred to the Agreement in the month of effective date. Subsequent payments will be calculated against all Subscribing Entities as stated above.

### **8. Appropriation and Certification of Funds**

#### **8.1. Appropriation of Funds.**

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails at any time to continue funding for the payments or any other obligations due from the State under this Agreement, the State will be released from its obligations on the date funding expires.

#### **8.2. Certification of Funds**

None of the rights, duties, or obligations in this Agreement will be binding on the State or a Subscribing Entity, and the Service Provider will not begin its performance under any Order, until all the following conditions occur for that Order: (a) all statutory provisions under the ORC, including Section 126.07, have been met; (b) all necessary funds are made available by the appropriate State agencies; (c) if required, approval of this Agreement or the applicable Order is given by the Controlling Board of Ohio; and (d) if the Subscribing Entity is relying on federal or third-party funds for its Order, the Subscribing Entity gives the Service Provider written notice that such funds have been made

## MASTER CLOUD SERVICES AGREEMENT

available. Additional or alternate legal requirements may apply to political subdivisions that are a Subscribing Entity for an Order to be binding on it.

### 9. Support

#### 9.1. Maintenance and Support Generally

During the term of any Order, the Service Provider will provide the State with maintenance and support in connection with the SaaS Software as provided in Sections 1.24 and 5.1 of the attached EULA. Remedies for nonconformities with respect to maintenance and support are set forth in Section 10.5 of the attached EULA.

#### 9.2. Minimum Availability

Minimum availability shall be as set forth in Section 6.2 of the attached EULA. Section 10.4 of the attached EULA provides all remedies related to availability.

#### 9.3. Support Parameters

The parameters for support for the SaaS Software shall be as set forth in Sections 1.24 and 5.1 of the attached EULA pursuant to the M&S Specifications, as defined in Section 1.23 of the EULA. The current version of the M&S Specifications is attached as an exhibit of the Service Attachment. Further, the Service Provider must maintain at least one support center in North America with adequate English-speaking support personnel.

#### 9.4. Incident Classification

Incident Classification in connection with the SaaS Software shall be as set forth in Section 6.3 of the attached EULA.

#### 9.5. Incident Response

Incident Responses in connection with the SaaS Software shall be as set forth in Section 6.4 of the attached EULA.

#### 9.6. Response Times

Incident Response Times in connection with the SaaS Software shall be as set forth in Section 6.4 of the attached EULA.

#### 9.7. Escalation Process

The Escalation Process in connection with the SaaS Software shall be as set forth in M&S Specifications, as defined in Section 1.23 of the attached EULA, the current version of which is attached as an exhibit of the Service Attachment.

#### 9.8. State Obligations

To facilitate the Service Provider meeting its support obligations, the State must provide the Service Provider with the information reasonably necessary to determine the proper classification of the underlying problem. It also must assist the Service Provider as reasonably necessary for the Service Provider's support personnel to isolate and diagnose the source of the problem. Additionally, to assist the Service Provider's tracking of support calls and the resolution of support issues, the State must make a reasonable effort to use any ticket or incident number that the Service Provider assigns to a particular incident in each communication with the Service Provider.

## MASTER CLOUD SERVICES AGREEMENT

### 9.9. Relationship to SLAs

The Service Provider's support obligations are in addition to the SLAs in the Service Attachment(s). Furthermore, if agreed to by the Service Provider, the SLAs may provide for credits to the Subscribing Entities even though the Service Provider is meeting its support obligations hereunder.

## 10. Standard Provisions

### 10.1. Excusable Delay

Neither Party will be liable for any delay in its performance that arises from causes beyond its control and without its negligence or fault. The delayed Party will notify the other promptly of any material delay in performance and will specify in writing the proposed revised performance date or dates as soon as practicable after notice of delay. The proposed date or dates must be reasonable and cannot exceed the actual delay caused by the events beyond the control of the Party. In the case of such an excusable delay, the dates of performance or delivery affected by the delay will be extended for a period equal to the time lost by reason of the excusable delay. The delayed Party must also describe the cause of the delay and what steps it is taking to remove the cause. The delayed Party may not rely on a claim of excusable delay to avoid liability for a delay if the delayed party has not taken commercially reasonable steps to mitigate or avoid the delay. Things that are controllable by the Service Provider's suppliers will be considered controllable by the Service Provider.

In the case of SaaS Licenses for a term that an excusable delay interrupts, the term of that SaaS License will be extended at no additional cost to affected Subscribing Entities by the same amount of time as the excusable delay.

### 10.2. Employment Taxes

Each Party will be solely responsible for reporting, withholding and paying all employment related taxes, contributions and withholdings for its own personnel, including, but not limited to, federal, state, and local income taxes, and social security, unemployment and disability deductions, withholdings, and contributions, together with any interest and penalties.

### 10.3. Sales, Use, Excise, and Property Taxes

The State and most Subscribing Entities are exempt from any sales, use, excise, and property tax. To the extent sales, use, excise, or any similar tax is imposed on the Service Provider in connection with the SaaS Software or any professional services, such will be the sole and exclusive responsibility of the Service Provider, and the Service Provider will pay such taxes (together with any interest and penalties not disputed with the appropriate taxing authority) whether they are imposed at the time the Services are rendered or a later time.

### 10.4. Equal Employment Opportunity

The Service Provider will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including ORC Section 125.111 and all related Executive Orders.

Before this Agreement can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the DAS Equal Opportunity Division to comply

## MASTER CLOUD SERVICES AGREEMENT

with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by to the Ohio Business Gateway at:

<http://business.ohio.gov/efiling/>

The State encourages the Service Provider to purchase goods and services from Minority Business Enterprises ("MBEs") and Encouraging Diversity, Growth and Equity ("EDGE") contractors.

### 10.5. Drug-Free Workplace

The Service Provider must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Service Provider must make a good faith effort to ensure that all its employees, while working on State property or the property of any Subscribing Entity, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.

### 10.6. Conflicts of Interest

No Service Provider personnel may voluntarily acquire any personal interest that conflicts with the Service Provider's responsibilities under this Agreement. Additionally, the Service Provider will not knowingly permit any public official or public employee who has any responsibilities related to this Agreement or the Project to acquire an interest in anything or any entity under the Service Provider's control, if such an interest would conflict with that official's or employee's duties. The Service Provider will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Agreement. The Service Provider will take all legal steps to ensure that such a person does not participate in any action affecting the work under this Agreement, unless the State has determined that, in the light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.

### 10.7. Assignment

The Service Provider may not assign this Agreement or any of its rights or obligations under this Agreement without the prior, written consent of the State, which consent the State will not be obligated to provide.

### 10.8. Governing Law

This Agreement will be governed by the laws of Ohio, and venue for any disputes will lie with the appropriate court in Ohio.

### 10.9. Finding for Recovery

The Service Provider warrants that the Service Provider is not subject to an unresolved finding for recovery under ORC §9.24. If the warranty is false on the date the parties signed this Agreement, the Agreement is void *ab initio*.

### 10.10. Anti-trust

The Parties recognize that, in actual economic practice, overcharges resulting from antitrust violations are usually borne by the State and the Subscribing Entities. The Service Provider therefore assigns to the State all state and federal antitrust claims and causes of action that the Service Provider now has or may acquire relating to the SaaS Software arising in relation to the terms and conditions of this Agreement.

## **MASTER CLOUD SERVICES AGREEMENT**

### **10.11. Use of Name**

Neither Party will use the other Party's name in any marketing material, advertisement, or press release without the other Party's written consent. Further, neither Party may use any contact information collected from the other in the performance of this Agreement for general marketing or sales purposes, such as using email addresses to send mass marketing material, and must use such information solely for purposes of administering this Agreement.

### **10.12. Executive Order 2011-12K Compliance**

The Service Provider affirms to have read and understands Executive Order 2011-12K and will abide by those requirements in the performance of this Agreement. The Service Provider has a sister company domiciled in India called AirWatch Technologies India Private Limited that may provide programming resources in connection with the SaaS Software or Maintenance and Support and may provide professional services. The State hereby waives its rights with respect to AirWatch Technologies India Private Limited. Notwithstanding any other terms of this Agreement, other than with respect to AirWatch Technologies India Private Limited, the State reserves the right to recover any funds paid for SaaS Software and any professional services performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights and remedies provided the State in this Agreement.

The Service Provider agrees to complete the attached Executive Order 2011-12K Affirmation and Disclosure Form which is incorporated and becomes a part of this Agreement.

### **10.13. Campaign Contributions**

The Service Provider, by signature affixed on this document, hereby certifies that all applicable parties listed in O.R.C. Section 3517.13 are in full compliance with O.R.C. Section 3517.13.

### **10.14. Declaration Regarding Terrorist Organization**

The Service Provider represents and warrants that is has not provided any material assistance, as that term is defined in ORC Section 2909.33(C), to an organization that is identified by, and included on, the United States Department of State Terrorist Exclusion List and that it has truthfully answered "no" to every question on the DMA form. The Service Provider further represents and warrants that it has provided or will provide the DMA form through the Ohio Business Gateway at <http://business.ohio.gov/efiling/> prior to execution of this Agreement. If these representations and warranties are found to be false, this Agreement will be void and the Service Provider will immediately repay to the State any funds paid under this Agreement.

### **10.15. Export Compliance**

The Services and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Both the Service Provider and the State represent that it is not named on any U.S. government denied-party list. Neither party will permit others to access or use the Services in a US-embargoed country (currently Cuba, Iran, North Korea, Sudan or Syria) or in violation of any U.S. export law or regulation.

## **MASTER CLOUD SERVICES AGREEMENT**

### **10.16. Safety and Security Rules**

When accessing State networks and systems, the Service Provider must comply with all applicable State policies and regulations regarding data security and integrity. And when on any property owned or controlled by the State, the Service Provider must comply with all security and safety rules applicable to people on those premises. Subscribing Entities may have policies and regulations that are specific to them that the Service Provider also must comply with.

### **10.17. Ohio Ethics Law**

The Service Provider certifies that it is currently in compliance and will continue to adhere to the requirements of the Ohio ethics laws.

### **10.18. Entire Agreement**

This Agreement, together with the attached EULA, any Service Attachments, and all additional documents expressly incorporated herein, sets forth the entire agreement of the Parties with respect to the subject matter hereof and supersedes any prior agreements, promises, representations, understandings, and negotiations between the Parties with respect to the subject matter hereof.

Only executable Order Forms attached to a Service Attachment as an exhibit and identified as such in the applicable Service Attachment may be executed by a Subscribing Entity to evidence a transaction under this Agreement, though a Subscribing Entity may issue its own purchasing forms, such as a purchase order. Further, the Subscribing Entity may not add or require additional terms as part of any authorized form. Documents attached to a Service Agreement as exhibits to be executed by a Subscribing Entity typically identify authorized Service options the Subscribing Entity has selected, provide information about a Subscribing Entity, identify installation or configuration requirements or similar statements of work to be done by the Service Provider, set schedules for performance, and similar matters.

### **10.19. Severability**

If any provision hereunder is declared or held invalid, illegal, or unenforceable by a court of competent jurisdiction, this Agreement will be revised only to the extent necessary to make that provision legal and enforceable or, if impossible, the unaffected portions of this Agreement will remain in full force and effect so long as the Agreement remains consistent with the Parties' original intent.

### **10.20. Survival**

Any terms, conditions, representations, or warranties contained in this Agreement that must survive termination or expiration of this Agreement to be fully effective will survive the termination or expiration of the Agreement, unless expressly provided otherwise in this Agreement. Additionally, no termination or expiration of the Agreement will affect the State's right to receive the benefits of the SaaS software or professional services for which the State has paid before expiration or termination, but no subscription to the SaaS Software will continue beyond the period paid for before termination or expiration of the Agreement.

If any Service Attachment should expire or be terminated, the remaining portions of this Agreement will survive.

## **MASTER CLOUD SERVICES AGREEMENT**

### **10.21. No Waiver**

The failure of either party at any time to demand strict performance by the other Party of any terms or conditions of this Agreement may not be construed as a waiver of any of those terms or conditions, and either Party may at any time demand strict and complete performance by the other Party.

### **10.22. Order of Precedence**

It is the express agreement of the Parties that the Order of Precedence shall be: 1) Master Cloud Service Agreement; 2) Service Attachment; and 3) End User License Agreement. In the case of any conflict, the order of precedence shall be as stated above. Sections 7.5, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, and 9.7 of the MCSA make references to specific sections of the EULA. The Parties agree that those sections will be considered to fall under item 2 (EULA) in the Order of Precedence. In the case of any conflicting provision in the Service Attachment will be applicable only to that Service Attachment and then only to the Services thereunder that are intended to be covered by that provision. But if any such action materially affects any Subscribing Entity's use of a Service, the Subscribing Entity may on written notice to the Service Provider terminate its use of the Service without an Early Termination Charge and receive a pro rata refund any amounts paid in advance for the Service.

### **10.23. Headings**

The headings herein are for convenience only and are not intended to have any substantive significance in interpreting this Agreement.

### **10.24. Governmental Authorization, Regulatory Changes**

This Agreement is subject to all applicable federal, state, and local laws, rules, orders, and regulations, and each Party must comply with all applicable federal, state, and local laws, rules, regulations, and orders in performing its obligations hereunder. To the extent any provision of this Agreement conflicts with any such applicable law, rule, order, or regulation, such law, rule, order, or regulation will supersede the conflicting provision. The Service Provider may discontinue, limit, or impose additional requirements to the provision of the SaaS Software, upon no less than 30 days written notice, if required to meet federal, state, or local laws, rules, or regulations.

### **10.25. Notices**

Except as otherwise provided in this Agreement, all notices hereunder must be in writing and sent by (a) registered or certified mail, postage prepaid; (b) facsimile transmission; (c) overnight courier; (d) or email, upon confirmation of receipt. Alternatively, such notices may be hand delivered if confirmation of receipt is attained at delivery.

The State's address for notification is:

Department of Administrative Services  
Office of Information Technology  
Infrastructure Services Division  
1320 Arthur E. Adams Drive, 3rd Floor  
Columbus, Ohio 43221  
Attention: Contract Manager

With a copy to:

**MASTER CLOUD SERVICES AGREEMENT**

Department of Administrative Services

Office of Legal Services

30 East Broad Street, 40<sup>th</sup> Floor

Columbus, Ohio 43215

Attention: Chief Legal Counsel

The Service Provider's address for notification is:

AirWatch, LLC

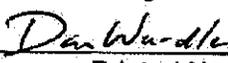
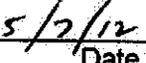
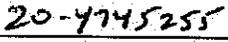
931 Monroe Drive, Suite 102-303

Atlanta, GA 30308

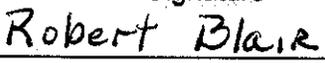
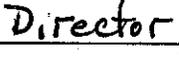
ATTN: Legal

IN WITNESS WHEREOF, the Parties have executed this Agreement on the dates indicated below.

**SERVICE PROVIDER:  
AIWATCH, LLC**

  
\_\_\_\_\_  
Signature  
  
\_\_\_\_\_  
Printed Name  
  
\_\_\_\_\_  
Title  
  
\_\_\_\_\_  
Date  
  
\_\_\_\_\_  
Federal Tax ID

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

  
\_\_\_\_\_  
Signature  
  
\_\_\_\_\_  
Printed Name  
  
\_\_\_\_\_  
Title  
  
\_\_\_\_\_  
Effective Date

