

SERVICE ATTACHMENT 3 CLOUD SERVICES

This Service Attachment (the "Service Attachment"), is between **Bluemile, Inc.** ("Service Provider") having an office at 7775 Walton Parkway, New Albany, Ohio 43054, and **the State of Ohio, Department of Administrative Services,** ("the State"), having its principal place of business at 30 E. Broad St. – 40th Floor, Columbus, Ohio 43215 (jointly referred hereto as the "Parties"), and it is effective as of the date signed by the State. This Service Attachment is entered into, subject to, and incorporates by reference the terms and conditions of, that certain Master Services Agreement between the Parties dated June 5, 2012 (the "MSA"). Capitalized terms used herein without definition shall have the respective meanings ascribed to them in the MSA or elsewhere in this document. Agencies boards, commissions and Cooperative Purchasing members who purchase under this Agreement with Service Provider will be known as Subscribing Entities.

1. Service Overview

Bluemile (Service Provider) provides Cloud Computing Services (hereinafter referred to as "Cloud Services") of which Subscribing Entities can take advantage. Cloud Services allow Subscribing Entities to utilize the infrastructure and services of Service Provider's facilities for compute, disk, backup and other related services.

2. Description of Service

Cloud services supplied by Service Provider offer a broad array of computing Services for Subscribing Entities. The Virtual Data Center (VDC) is a combination of Compute and Storage Cloud Services. This is a managed environment. Bluemile Infrastructure as a Service (IaaS, Cloud Services) includes:

- Compute – provides a virtual server(s) that may be used by Subscribing Entities just as they would a physical server(s) deployed in their data center. Service Provider bills compute resources hourly based on virtual machine configuration and use. The Subscribing Entity's authorized administrators can create or delete guest systems as needed.
- Storage – allows for the Compute process to have a location to store applications and data. Service Provider bills on an hourly basis, based on monthly commitments for storage, which is can be found in Section 5 of this Service Agreement. There are three different performance tiers: Near Line (SATA drives), Performance (high-speed fiber channel drives) and Extreme (Solid State technology of no less than 500 MB/s aggregate read/write speed). Collocation and Transport Subscribing Entities may also access Storage directly through Service Provider provided local storage connectivity.
- Backup – provides Subscribing Entities with a backup functionality that is stored off site at a secure Service Provider facility. Service Provider will invoice backup(s) based on the storage used per month and pricing which can be found in Section 5 of this document.
- Replication – provides Subscribing Entities with a means of facilitating environment disaster recovery. Replication provides Storage and/or Compute replication between a primary and secondary site (utilizing both Service Provider data centers). If a single site is unavailable as a result of a disaster, then the secondary site is available with the actively replicated data and virtual machines available. Replication services will be implemented as to ensure that no more than 24 hours of processing are lost (Recovery Point Objective) and Services are transferred to the replication site no less than 48 hours from the time of the disaster affecting the primary Service Provider data center

SERVICE ATTACHMENT 3 CLOUD SERVICES

(Recovery Time Objective). Replication bills based on GB of storage or MB of RAM leveraged per month as detailed in Section 5.

In the Cloud Services (IaaS) model, Subscribing Entities are given access to their VDC environment and the Subscribing Entity is responsible for the creation and deletion of managed guest systems. As an optional service, Bluemile Managed Services can perform these tasks.

3. Optional Services

There are also Optional Services that Subscribing Entities can purchase as part of Cloud Services. These Optional Services allow Subscribing Entities to expand the basic services beyond what is available from the cloud.

The following are Optional Services the Service Provider offers for Cloud Services. Pricing for these services resides in Section 5.3:

- Managed Firewall – Allows Service Provider to manage the firewall configuration and service updates as requested by Subscribing Entity.
- Managed IDS/IPS – Service Provider provides all maintenance and configuration of the Intrusion Detection System (IDS)/Intrusion Prevention System (IPS). IDS/IPS systems provide protection to networks by detecting and to the extent possible utilizing the Service Provider's implemented network devices, preventing attacks. In most cases, the Subscribing Entity will review and resolve the IDS/IPS events, but the IDS/IPS events that cannot be resolved can be triaged and prioritized before the event is sent to the Subscribing Entity for review/resolution.
- Monitoring – provides a view as to the status, performance and availability of the systems in the Subscribing Entity's contracted environment by providing reporting, alerting, and feedback to the Subscribing Entity. Monitoring will provide the ability to consolidate data from VMWare, Operating system, Storage and associated Networks (wide area or storage), and other sources into one single integrated view of the Subscribing Entities contracted environment.
- Managed Load Balancing – Subscribing Entities can leverage a load balanced environment managed by the Service Provider. Load balancing allows alternating servers to share load across multiple systems.
- Managed VPN – Service Provider can offer Subscribing Entities a managed VPN connection that Service Provider provides and maintains.

Due to the fluid nature of the Optional Services many are provided on an Individual Case Basis.

4. Fee Structure

The Service Provider is providing the following pricing to deliver its Cloud Services to the Subscribing Entities. The pricing includes monthly Cloud Pricing, One-Time or Non-Recurring Charges (NRC), and the Term of an Order placed in the State Ordering System. Cloud price covers the Services that this Service Attachment defines which the Service Provider provides to the Subscribing Entity. The NRC covers costs of provisioning the

SERVICE ATTACHMENT 3 CLOUD SERVICES

services. All charges are governed by the Term, which provides the length of the Services contract. Additional charges might be incurred for optional services requested, but will not be billed without an approved Order placed in the State's Ordering System.

The Service Provider provides services to the Subscribing Entity based upon minimum commitment levels for the core services and duration. The Subscribing Entity will be billed at this level, whether the services are being consumed or not. The Service Provider will configure the VDC so that the Subscribing Entity may exceed its minimum commitment level by 25% for Storage. Due to technical limitations, the Service Provider cannot set limits on compute. Therefore, the Service Provider will send a notification to the Subscribing Entity when usage is 25% above the commitment level. If notification is not sent to the Subscribing Entity at 25%, but is sent at a higher percentage, the Subscribing Entity will be credited the difference percentage the higher percentage and the 25%. For example, if Subscribing Entity is notified of usage at 30% above commitment level, then the Subscribing Entity will be responsible for the first 25%, will be credited the next 5% and then will be responsible for all usage at 30% and above. This allows for growth and flexibility. Billing for any usage over the commitment level is determined on an hourly basis based upon the corresponding hourly price for a given service as per pricing in Section 5.

For example, a Subscribing Entity that has contracted Compute and Storage for four (4) virtual machines of 4 GB RAM and 1 TB drive space each would have a monthly commitment level of 16 GB RAM (Compute) and 4 TB of drive space (Storage). The Subscribing Entity would be able to expand that environment up to 4 GB RAM and 5 TB of storage. This allows for temporarily or permanently creating new systems to handle requirements as they arise. It is also possible for Subscribing Entities to increase the amount of processing power within their virtual machines above that default amount provided. This incurs an additional per hour charge as per pricing schedules in Section 5.

**SERVICE ATTACHMENT 3
CLOUD SERVICES**

5. Pricing Schedules

5.1. Virtual Data Center Monthly Rates (Compute and Storage)

This is the monthly pricing for Compute and Storage for the Virtual Data Center.

Virtual Data Center Monthly Rates (Compute and Storage)

Virtual Data Center Monthly Rates				
Service	Non-Recurring Charge	12 Month Contract Monthly Recurring Charge (MRC)	24 Month Contract MRC	36 Month Contract MRC
RAM (Compute, per GB)	ICB	\$41.12	\$30.84	\$27.41
Extreme Storage (Solid State Drive, per GB)	ICB	\$0.5050	\$0.475	\$0.400
Performance Storage (15k Fiber Channel, per GB)	ICB	\$0.2520	\$0.23	\$0.200
Near Line Storage (SATA, per GB)	ICB	\$0.198	\$0.185	\$0.165
CPU per hour* (Unix/Linux/Windows)	ICB	\$0.091553	\$0.074907	\$0.066584

* CPU per hour is measured by productive use by the State of a provided CPU of no less than 4 virtual cores. Productive use is defined as performance of computing work for the State and exclusive of machine idle time.

SERVICE ATTACHMENT 3 CLOUD SERVICES

5.2. Cloud Services Backup Service

This is the pricing for various backup offerings for Cloud Services.

Backup Services

Backup Services				
Service	Non-Recurring Charge	12 Month Contract Monthly Recurring Charge (MRC)	24 Month Contract MRC	36 Month Contract MRC
Virtual Machine Disaster Recovery Backup (per VM*)	ICB	\$100.00	\$80.00	\$75.00
Off-Site Backup Service (per GB vaulted)	\$250.00*	\$0.198	\$0.185	\$0.165
NFS Archive (per GB)	\$250.00*	\$0.198	\$0.185	\$0.165
Data Domain© Target Services (per GB)	\$250.00*	\$0.125	\$0.125	\$0.125

*Client will be billed for amount of storage used on backup VM system for system to lie idle waiting for the fail-over. Customer will not be billed for CPU or RAM unless a fail over is invoked.

5.3. Optional Services for Cloud

This is the pricing for an Optional Cloud Services for the 12, 24, and 36 month Terms.

Optional Cloud Services

Optional Cloud Services				
Service	Non-Recurring Charge	12 Month Contract Monthly Recurring Charge (MRC)	24 Month Contract MRC	36 Month Contract MRC
Unmanaged Firewall up to 100 Mbps	\$200.00	\$250.00	\$196.00	\$181.00
Unmanaged Firewall 101 Mbps up to 1 Gbps	\$275.00	\$1000.00	\$783.00	\$722.00
Unmanaged Firewall 1+ Gbps	ICB	ICB	ICB	ICB
Managed Firewall* up to 100 Mbps	\$350.00	\$350.00	\$296.00	\$281.00
Managed Firewall* 101 Mbps up to 1 Gbps	\$350.00	\$1100.00	\$883.00	\$822.00

**SERVICE ATTACHMENT 3
CLOUD SERVICES**

Optional Cloud Services				
Service	Non-Recurring Charge	12 Month Contract Monthly Recurring Charge (MRC)	24 Month Contract MRC	36 Month Contract MRC
Managed Firewall* 1+ Gbps	ICB	ICB	ICB	ICB
Unmanaged Load Balancing* up to 100 Mbps	\$350.00	\$250.00	\$196.00	\$181.00
Unmanaged Load Balancing* 101 Mbps up to 1 Gbps	\$350.00	\$1000.00	\$783.00	\$722.00
Unmanaged Load Balancing* 1+ Gbps	ICB	ICB	ICB	ICB
Managed Load Balancing* up to 100 Mbps	\$350.00	\$350.00	\$296.00	\$281.00
Managed Load Balancing* 101 Mbps up to 1 Gbps	\$350.00	\$1100.00	\$883.00	\$822.00
Managed Load Balancing* 1+ Gbps	ICB	ICB	ICB	ICB
Host Monitoring (up to 25 hosts, prices per host)	\$25.00	\$102.95	\$71.00	\$63.90
Host Monitoring (26-51 hosts, price per host)	\$25.00	\$98.60	\$68.00	\$61.20
Host Monitoring (51-100 hosts, price per host)	\$25.00	\$92.80	\$64.00	\$57.60
Host Monitoring (101+ hosts, per host)	\$25.00	ICB	ICB	ICB
Managed VPN Connection (1 IPSec Tunnel)	\$125.00	\$143.55	\$99	\$89.10
Managed IDS up to 50 Systems	\$1,000.00	\$720.00	\$600.00	\$576.00
Managed IDS 51 up to 100 Systems	\$1,133.33	\$1,520.00	\$1,266.67	\$1,216.00
Managed IDS 101 up to 250 Systems	\$1,466.67	\$1,920.00	\$1,600.00	\$1,536.00
Managed IDS 251 up to 500 Systems	\$1,600.00	\$2,080.00	\$1,733.33	\$1,664.00
Managed IDS 501 up to 1000 Systems	\$1,866.67	\$2,400.00	\$2,000.00	\$1,920.00
Managed IDS 1001 up to 1500 Systems	\$2,400.00	\$3,200.00	\$2,666.67	\$2,560.00
Managed IDS 1501 up to 2000 Systems	\$2,933.33	\$3,840.00	\$3,200.00	\$3,072.00

**SERVICE ATTACHMENT 3
CLOUD SERVICES**

Optional Cloud Services				
Service	Non-Recurring Charge	12 Month Contract Monthly Recurring Charge (MRC)	24 Month Contract MRC	36 Month Contract MRC
Managed IDS 2001 up to 2500 Systems	\$3,866.67	\$5,120.00	\$4,266.67	\$4,096.00
Managed IDS w/ ActiveWatch up to 50 Systems	\$1,000.00	\$1,360.00	\$1,133.33	\$1,088.00
Managed IDS w/Protect Watch 51 up to 100 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 101 up to 250 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 251 up to 500 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 501 up to 1000 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 1001 up to 1500 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 1501 up to 2000 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB
Managed IDS w/Protect Watch 2001 up to 2500 Systems	\$ ICB	\$ ICB	\$ ICB	\$ ICB

* Managed Firewall and Load Balancing includes monthly configuration changes, not to exceed 2 hours of effort. Additional hours are available at \$150/hour.

Note: Managed IDS/IPS includes monthly configuration changes, not to exceed 2 hours of effort. Additional hours are available at \$150/hour. Managed IDS/IPS does not include monitoring and managing alerts, only the system and rules defined.

**SERVICE ATTACHMENT 3
CLOUD SERVICES**

5.4. Professional Services Schedule of Services. The following table provides the fees associated with various professional services offerings available.

Professional Service Resource	Hourly Rate*	After Hour Rate**	Minimum Commitment	Billing Increment
NOC Service Technician	\$90.00	\$135.00	1 hour	30 minute
Field Service Technician	\$125.00	\$187.50	1 hour	30 minute
Network Engineer	\$225	\$400	1 hour	30 minute
Security Engineer	\$250	\$450	1 hour	30 minute
Network Operations Project Manager	\$225	\$400	8 hour	1 hour

* Hourly rates are for normal business hours, 8 AM – 5 PM EST Monday through Friday.

** After hours, weekends, and holiday rates. Service Provider holidays include: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Friday after Thanksgiving Day, Christmas Eve Day, Christmas Day, and New Year's Eve Day.

5.5. Cloud Services pricing schedule include several payment options.

- (A) The Subscribing Entity pays for the NRC and NRCC after the work is performed at the beginning of the contract. All MRCs are paid on the billing due date.
- (B) The Service Provider may offer the Subscribing Entity with an option to amortize the NRC and NRCC over a period of time, not to exceed the Term of the contract for Services. This option may include a management fee to cover the cost of managing the NRC and NRCC. MRCs are due on the billing due date.

6. Terms & Conditions

The MSA describes many of the common terms and conditions. Terms and conditions in this Service Attachment pertain to the Cloud Services described in this document. Early Termination charges for any cancelled Cloud Service shall equal the sum of:

- (A) Fifty percent (50%) of all unpaid amounts for Service(s) provided through the date of termination; plus
- (B) any documented termination liability payable to appropriate third parties resulting from the termination (third-parties may include carriers like; VMware, Microsoft) plus the lesser of
- (C) for each minimum volume requirement remaining on the contracted Term (the "MVR"), 50% of any and all corresponding minimum volume commitments and charges, less amounts previously paid by Subscribing Entity toward that specific MVR (the MVR is the minimum amount of a total contract by a Subscribing Entity with the Service Provider); or
- (D) In the event no MVR is stated in a given service order within the State's Ordering System, 50% of the monthly recurring charges at rates defined above for all months remaining in the applicable Service Order Form (SOF) Term.

SERVICE ATTACHMENT 3 CLOUD SERVICES

Logically this would work out to be: A + B + (C or D)

Early Termination Charges. Early Termination charges do not apply in the event of non appropriation of funds or if Bluemile is in default based on the Terms of the Master Service Agreement.

Expedite Fees. If the Subscribing Entity wishes to speed the acquisition of services they may consider Expedite Fees. These are the costs associated with expediting the installation of a Service which may include a per item charge. These fees will be presented at the time of pricing request. Service Provider reserves the right to determine if it can accommodate an expedite installation request. There may be an ICB quote provided to meet the expedited Service. Subscribing Entity must include the expedite quote in any Order placed requiring such service.

Additional Services. It is possible for the Subscribing Entity to add Additional Services. This is done through the State's Ordering System. Subscribing Entities may add Services: (a) during the Term of the initial order, staying within that Term, or (b) during the initial Term and extend the Term of the applicable Order. The price will be determined in this Service Attachment to the nearest full length of billing term remaining. For example, if an entity with a thirty-six (36) month contract wants to add storage in month twenty-three (23), the nearest pricing that allows for the full term is the twelve (12) month pricing limit ($36 - 23 = 13$, which is less than 24 months, but greater than 12.) Likewise, adding storage in the 15th month of a thirty-six (36) month contract would require the twenty-fourth (24) month term pricing for the remainder of the term ($36 - 10 = 26$, which is greater than 24 but less than 36.) Service Provider and Subscribing Entity may extend the existing contract Term to match the new Service Term if mutually agreeable.

Change Services. Subscribing Entities may also change Services subject to this Service Attachment and the MSA. The service type may change to meet changes needed by the Subscribing Entity with a minimum of thirty (30) days written notice. The new MRC is based on the service contract to the nearest full term of billing remaining on the contract. Change in service type might require additional NRC or other costs, which are evaluated on an ICB. Additionally, changing the Subscribing Entity to a lower cost service may invoke Early Termination charges as described in the MSA unless mutually agreed upon by both parties.

7. **Service Level Agreement and Schedule of Credits** - This Service Level Agreement (SLA) becomes effective upon initial confirmation of traffic passing into Subscribing Entity's Cloud Services environment by the Subscribing Entity. The beginning of the Service Level Agreement has no bearing on the start of billing for related services.

Cloud Availability

The Service Provider is committed to providing the highest availability to the Subscribing Entities. The Service Provider's SLA for Cloud Availability for all Cloud Services provided by Bluemile is 99.95% as measured on a 24 hour basis, 7 days per week, less mutually agreed upon scheduled outages.

The Service Providers Cloud Availability is defined as the percentage of minutes in a in any 30-day period a Subscribing Entity's Cloud Environment did not experience a Service Outage in that time period. Cloud Availability as a percentage is calculated:

SERVICE ATTACHMENT 3 CLOUD SERVICES

1 – (Time to restore service for all cloud outages in a billing period /Total minutes in the same period) x 100

The availability SLA does not account for scheduled outages on Service Provider's resources nor from Subscribing Entity issues or events outside of the Service Provider's control, including, but not limited to, force majeure events or Subscribing Entity managed environment outages. Cloud downtime is calculated commencing with the date and time on which the Subscribing Entity contacts the Service Provider and a trouble ticket is opened, and ending upon documented confirmation from the Service Provider that the Service is restored.

Severe And Chronic Problems

A Subscribing Entity is experiencing a Severe Problem if the aggregate Service Outage time or Service out of Specification Time experienced is in excess of twenty-four (24) hours in any rolling 30-day period. If a subsequent Severe problem occurs within the rolling 30-day period in which a Subscribing Entity experienced a Severe Problem, the problem will be considered Chronic. In the case of a Chronic problem, a full credit for the monthly services impacted by the Chronic problem shall be issued on the bill in the month immediately following the Chronic problem. In the case of a persistent Chronic problem, defined as those Chronic problems occurring in any three (3) consecutive months or in any three (3) months during a six month period, the State may terminate the services without penalty or cost in consideration of remaining Term of the Agreement.

Force Majeure

See Section 3.1 of the MSA.

Credit Availability

It is the Subscribing Entity's responsibility to identify and request all valid SLA claims and corresponding credits. To be eligible for Service credits, the Subscribing Entity must first report outage or Service out of specification events to Bluemile's National Support Center at 1-866-384-7587 while following prompts to submit a trouble ticket. Please request a ticket number from the Bluemile representative. The Bluemile will notify Subscribing Entity of its resolution of the reported outage. Bluemile Accounts Receivable will apply the credit arising from the SLA violation to the Subscribing Entity's next monthly invoice.

Service Outage

For purposes of this Service Attachment, a "Service Outage" will mean an unavailability of the Service to carry traffic between two points of Service, provided that a Service Outage will not be deemed to have occurred in the event that it arises from or relates to any of the following:

- (i) a circuit has not been accepted by Subscribing Entity;
- (ii) the negligence, error, acts or omissions of Subscribing Entity or others authorized by Subscribing Entity to use the Service;
- (iii) failure of Subscribing Entity provided equipment;
- (iv) during any period in which Service Provider or its agents are not afforded access to the Services under Subscribing Entity's control where the access lines associated with the Service are terminated;
- (v) during any period when Subscribing Entity and Service Provider have agreed to maintenance or rearrangement purposes (including, without limitation, during any Routine or Emergency Network Maintenance);
- (vi) any period when Subscribing Entity elects not to release the Service for testing and/or repair and continues to use it on an impaired basis;

SERVICE ATTACHMENT 3 CLOUD SERVICES

- (vii) an event where Service Provider's failure to perform is excused by the Subscribing Entity in writing;
- (viii) a breach by Subscribing Entity of its obligations under the MSA or this Service Attachment;
- (ix) Or the failure is the responsibility of a third-party, not provided by the Service Provider as part of the contracted Service that are outside of Service Provider's control.

8. **Maintenance**

Service Provider will occasionally have to perform **routine network maintenance** for network improvements and preventive maintenance. Service Provider will use reasonable efforts to provide 10 days notice to Subscribing Entities of all Routine Network Maintenance that could affect Subscribing Entities' Services and schedule the outage as to not impact or otherwise make unavailable the Subscribing Entities services during business hours. In some cases Service Provider will need to address Emergency Network Maintenance needs quickly in order to address serious security or performance concerns. In these situations all attempts will be made to provide a reasonable level of notice to Subscribing Entities about the upcoming changes and potential impacts. Emergency network Maintenance does not factor against SLA measurements as it is part of maintaining an efficient and secure operating environment.

The standard window for Routine Network Maintenance will be 12 AM until 6 AM local time Monday through Sunday. Notification will be provided by the Service Provider's Network Operations Center (NOC) to the contact listed for the Subscribing Entity. The notification will reference the start time, expected duration, proposed or required changes, and other pertinent information. Service Provider will internally devise and, if necessary, implement a backout strategy that may or may not be communicated to the Subscribing Entities. Service Provider reserves the right to conduct maintenance that requires a longer service window. Subscribing Entities will be informed and the Service Provider will endeavor to conduct longer service outages over weekends if possible.

It might be necessary to perform **Emergency Maintenance**. This might include important fixes for functionality or key security updates that need to be applied outside the standard Routine Maintenance Window described above. Service Provider will provide as much notice as is possible through email to contacts listed by the Subscribing Entities.

Subscribing Entities are required to enter service calls for Service outage issues they experience via Service Provider's 24x7x365 NOC. The Subscribing Entity should perform an initial analysis to ensure that the issue is not with the Subscribing Entity's system(s). Once it has been determined that the Subscribing Entity does not feel it is their issue, the Service Provider will perform an analysis. If the analysis indicates an issue is with the Subscribing Entity and not with the Service Provider, then the Service Provider may, at Service Provider's discretion, provide the Subscribing Entity with a bill for services on a time and material basis using Service Provider's current applicable rates defined in section 5.4

9. **Network Operations Center** - Service Provider maintains a Network Operations Center (NOC) staffed (24) hours per day, seven (7) days per week for the Subscribing Entity to open Service Tickets, receive status on existing tickets, and escalate issues when appropriate. Service Provider's staff is knowledgeable employees in the appropriate fields,

SERVICE ATTACHMENT 3 CLOUD SERVICES

the Service Provider's products, and services, and basic troubleshooting techniques. The Subscribing Entity NOC can be contacted at (866) 384-7587 or noc@bluemilenetworks.com.

- 10. Installation and Acceptance of Service** – In order for the Service Provider to successfully install the Services to a Subscribing Entity it is important for said Entity to obtain and maintain through the Term of any Services any consents, permits, or orders that are necessary to the efficient operation of the Services. This includes any landlord or land-owner permissions or exemptions or federal, state, or local permits, permissions, or exemptions.

The Service Provider personnel must be given reasonable access to facilities as necessary to install, deliver, operate, upgrade, or maintain the Services being provided and any equipment associated with those Services. The Service Provider will work with Subscribing Entities to perform work at a mutually agreeable time.

Subscribing Entities are also responsible for providing appropriate internal resources necessary to support, maintain, install, upgrade, or deliver the Services. This may include but is not limited to floor space, equipment rack space, personnel time, power, appropriate environmental controls, and others. The Service Provider will not unreasonably withhold access to a Subscribing Entity's access to the contracted space.

Subscribing Entity is responsible for ensuring the safety and security of any Service Provider equipment left on site for purposes of providing agreed upon Services.

Subscribing Entity will ensure that his/her site preparations are completed prior to Service Provider's installation or service call to the agreed upon schedule. Service Provider will make all reasonable efforts to complete installation or Service within agreed upon schedule and promptly notify the Subscribing Entity upon completion of the work, or if required that a delay will adversely impact the agreed upon schedule along with an revised schedule for completion.

Service Provider will provide a completion notice when the Service is completed and the Subscribing Entity has five (5) business days after receipt to either acknowledge or challenge the installation. Subscribing Entity must immediately notify Service Provider with sufficient detail if the Service is under-performing during the five (5) day Acceptance Period. Within thirty (30) days of the notice, the Service Provider will make all reasonable efforts to remedy the Service being provided. This process continues until the Service is accepted or rejected by the Subscribing Entity after the 30 day period. If the Subscribing Entity accepts the Service or fails to acknowledge the Service, then the Service is deemed accepted by the Subscribing Entity. The date of acceptance is referred to as the "service live date."

Subscribing Entity is responsible for connecting to the Service from the Service Provider CPE device. Subscribing Entity agrees that this Service Attachment and the MSA provide exclusive remedies to Service issues or failures.

- 11. Reporting** – Within thirty (30) days of the close of a quarter the Service Provider will provide a report to the State of Ohio that lists all of the Services associated with this Service Attachment that Subscribing Entities were using in the previous quarter. The report will be

SERVICE ATTACHMENT 3 CLOUD SERVICES

tabular and will include the following fields, if appropriate, at a minimum: Subscribing Entity, Service Type, Services Assigned,, Cloud Compute Charges, Cloud Storage Charges, Cloud Backup Charges, Managed Services Charges, Billing MRC, Invoice Number, Invoice Amount, Amount of Invoice Paid, Billing Account Number, Billing Contact, Billing Start Date, Site Contacts, Order Number, and potentially other information.

12. **Cost Recovery Fee (CRF)** – The Cost Recovery Fee is payable by the Service Provider to the State of Ohio. These fees are for the management and administration of the Services in the State's system. The Service Provider will generate a report within thirty (30) days of the end of each quarter. This report, described above, will provide details about the Services associated with this Service Agreement that were invoiced and paid within the previous quarter. The State of Ohio Department of Administrative Services will review the report against their records and generate an invoice for 2% of the Services paid during the preceding quarter. The Service Provider will pay the invoice for the quarterly Services paid as a Cost recovery Fee within 30 days of receipt.

13. Confidentiality

The State may disclose to the Service Provider 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 State delivers to the Service Provider will remain with the State. The Service Provider 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 State, or individuals or organizations about whom the State keeps information. The Service Provider may not disclose any Confidential Information to third parties and must use it solely to perform under this Agreement.

If any Service 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 State will keep all such Confidential Information in confidence and will not use it other than as authorized under this Agreement. Nor will the State disclose any such Confidential Information to any third party without first obligating the third party to maintain the secrecy of the Confidential Information.

If one party discloses Confidential Information ("Disclosing Party") to the other party to this Agreement ("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;

SERVICE ATTACHMENT 3 CLOUD SERVICES

- (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, item (3) in the preceding paragraph does not apply, and the Service Provider 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.

This Agreement is not Confidential Information. All its Terms and Conditions, including pricing and any attachments, represent public information.

SERVICE ATTACHMENT 3 CLOUD SERVICES

13.1. Public Records Requests.

Should the Service Provider receive any public records request with respect to any Subscribing Entity 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.

13.2. Handling of Subscribing Entity Data

"Subscribing Entity Data" is any information, data, files, or software that a Subscribing Entity uses or stores on or in conjunction with the Services, including but not limited to Generated Files. The Service Provider must use due diligence to ensure computer and telecommunications systems and Services involved in storing, using, or transmitting Subscribing Entity 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 services associated with Subscribing Entity Data.
- (5) Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with Subscribing Entity 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 Subscribing Entity 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,

SERVICE ATTACHMENT 3 CLOUD SERVICES

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 Subscribing Entity Data.

Unless a Subscribing Entity instructs the Service Provider otherwise in writing, the Service Provider must assume all Subscribing Entity Data is both confidential and critical for Subscribing Entity 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 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 Subscribing Entity Data, as well as attacks on the Service Provider's infrastructure associated with Subscribing Entity 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 Subscribing Entity Data.

The Service Provider must use appropriate measures to ensure that Subscribing Entity Data is secure before transferring control of any systems or media on which Subscribing Entity 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 Subscribing Entity 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 Subscribing Entity 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 Subscribing Entity Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls,

SERVICE ATTACHMENT 3 CLOUD SERVICES

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 will not load Subscribing Entity Data onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Agreement properly. Any encryption requirement identified in this provision must meet the NIST standards identified above.

The Service Provider must maintain an incident response capability for all security breaches involving Subscribing Entity 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 detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access Subscribing Entity Data or the infrastructure associated with Subscribing Entity Data.

In case of an actual security breach that may have compromised Subscribing Entity Data, including but not limited to loss or theft of devices or media, the Service Provider must notify the Subscribing Entity in writing of the breach within 24 hours of the Service Provider becoming aware of the breach, and fully cooperate with the Subscribing Entity to mitigate the consequences of such a breach. This includes any use or disclosure of the Subscribing Entity 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 affected Subscribing Entities full access to the details of the breach and assist each Subscribing Entity in making any notifications to potentially affected people and organizations that the affected Subscribing Entities deem are necessary or appropriate. The Service Provider must document all such incidents, including its response to them, and make that documentation available to the affected Subscribing Entities on request. In addition to any other liability under this Agreement related to the Service Provider's improper disclosure of Subscribing Entity Data, and regardless of any limitation on liability of any kind in this Agreement, the Service Provider will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Service Provider's possession. Such identity theft protection must be reasonably acceptable to the State.

SERVICE ATTACHMENT 3 CLOUD SERVICES

All Subscribing Entity Data will remain the property of the Subscribing Entity. The Service Provider must ensure that the Subscribing Entity retains access and download capability for purposes of retrieving its data for research, investigation, transfer, or migration to other systems.

All Subscribing Entity Data at rest in systems supporting the Service Provider's Services 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.

14. Disentanglement Service

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 any affected 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.

On request, the Service Provider will immediately provide a quote for such Disentanglement Services based on the rate(s) in the pricing table listed in 5.4 of this Service Attachment. Upon issuance of an Order for the Disentanglement Services, the Service Provider will immediately begin providing necessary and appropriate assistance to allow the Services to continue without interruption and to facilitate the transfer of the Services to the ordering Subscribing Entity or its designee ("Successor").

The Service Provider will provide the Disentanglement Services so that minimized risk and maximized 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.

All documents, processes, programs, and other tangible materials created by the Service Provider at any time during an Order or otherwise pursuant to the relationship will be the sole property of the applicable Subscribing Entity and must be delivered to the Subscribing Entity as well.

The Service Provider will assist the Subscribing Entity or the designated Successor 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.

SERVICE ATTACHMENT 3 CLOUD SERVICES

The Service Provider will participate in all disentanglement meetings as reasonably requested by the Subscribing Entity.

The Service Provider must return all of the Subscribing Entity's Data to the Subscribing Entity in accordance with the requirements of the previous section.

The Service Provider will take part in parallel operations and continue to perform the Service alongside resources supplied by the designated Successor or, as the case may be, the Subscribing Entity.

Additionally, the Service Provider will provide knowledge transfer for all incoming personnel who will assume responsibility for the Services 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.

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 also will provide the Subscribing Entity all information and documentation available regarding service delivery methods, processes, and issues related to the Subscribing Entity's use of the Service.

To the extent reasonably necessary to facilitate a smooth disentanglement, the Service Provider will provide the Subscribing Entity and any designated Successor, in writing, any applicable policies, practices, standards, processes, procedures, architectures, operating procedures, technical documentation and other documentation relating to the affected Services, and necessary access to the systems and locations from which the affected Services were provided.

The Service Provider will turn over any tools, software, equipment, and 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, the Service Provider will continue to provide the Service 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 Service under the applicable expired or terminated Order.

**SERVICE ATTACHMENT 3
CLOUD SERVICES**

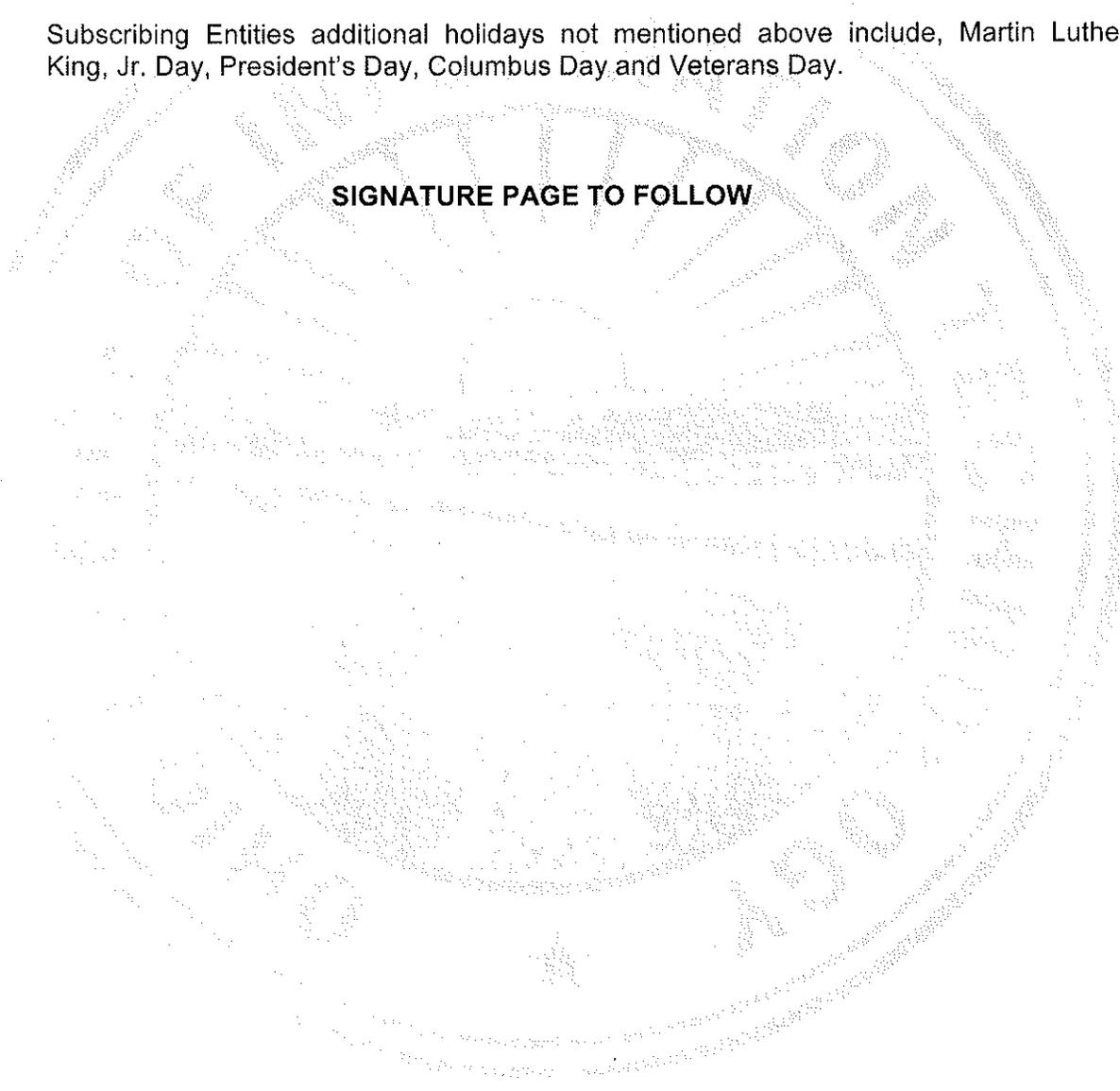
15. Holiday

Business Days exclude holidays.

Service Provider holidays include: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Friday after Thanksgiving Day, Christmas Eve Day, Christmas Day, and New Year's Eve Day.

Subscribing Entities additional holidays not mentioned above include, Martin Luther King, Jr. Day, President's Day, Columbus Day and Veterans Day.

SIGNATURE PAGE TO FOLLOW



**SERVICE ATTACHMENT 3
CLOUD SERVICES**

IN WITNESS WHEREOF, the Parties have executed this Service Attachment which shall be effective on the date signed by the State, "Effective Date."

BLUEMILE, INC.

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

Michael Manlove
Signature

Robert Blair/SRO
Signature

Michael Manlove
Printed Name

Robert Blair/Stuart Davis
Printed Name

President
Title

Dir/Asst Dir
Title

8/14/12
Date

8/20/12
Effective Date

20-4435654
Federal Tax ID

