Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

SERVICE AGREEMENT

between

The Maryland Department of Information Technology and

The Customer

for

Public Cloud Hosting Platform (Amazon Web Services)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I. Service Description

DoIT offers third-party compute and storage options with Amazon Web Services (AWS) as a standard model of cloud computing where IT services are provisioned over private IT hardware infrastructure for a customer organization. The public cloud infrastructure can be leveraged by a customer to host applications, storage and services over a networkMaryland™ provided private connection. The DoIT AWS cloud can provide a Commercial or Government hosting environment to suit client needs. Hybrid Cloud Hosting between Private and Public Cloud Hosting environments is also offered by DoIT.

A. Standard Service:

The following components are included with the standard service:

1. Assisting clients with the development of a work order. There are two types of work orders; a) one work order covers an estimation of AWS utilization rates based on what is hosted in the Public Cloud Hosting platform, and b) the other work order is to request professional contractual services to stand up a new service, application or perform a system migration or on premise transfer.
2. Work order modifications if costs will exceed currently executed work orders.
3. Onboarding and Account provisioning.
4. Deployment and configuration of a secure, standardized architecture that adheres to the Center for Internet Security (CIS) AWS Foundations Benchmark and the AWS Foundational Security Best Practices.

5. Enabling of cross-account access; VPC Network Setup; Classless Inter-Domain Routing (CIDR) IP address assignments from networkMaryland™
6. Creation of subnets, routing tables, virtual firewalls (NACL/Security Group), endpoints, NAT, Internet, and Virtual Private Gateways.
7. AWS Identity and Access Management (IAM) consists of setting up password policies, users, groups, roles and following resource naming and tagging standards.
8. Direct Connect setup to configure public and private virtual interface and VPN configuration.
9. Desktop Solution: Amazon Workspace
10. Security Operations which include a centralized security log management, anti-virus and vulnerability assessment
11. Develop cost estimates for Public Hosting services; Account billing and cost alerting; Guidance on AWS best practices and design.
12. Encryption for EBS volumes and S3 Buckets to be enabled upon request.
13. Administration and management of the Hosting Shared Services Web Application Firewall (WAF).
14. Assisting with initial design and requesting private lease connections over NetworkMD to public cloud. To extend existing NetworkMD services to AWS for a Hybrid network solution.
    a) Monitoring and alert notifications of NetworkMD circuits connecting to the public cloud.

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Firewall services that are not part of the web application firewall.
2. Customer application support including, but not limited to, websites and applications, databases, database administration, native database backup maintenance plans, COTs software applications, application upgrades or customizations and database encryption.
3. Access: DoIT will not provide console access to the virtual server or hypervisor console.
4. Agency's remote devices and services (i.e., any devices not hosted within MD DoIT's private cloud environment/data center).
    a) Examples include physical or virtual servers, hypervisors, scanning devices, storage devices, server backup system, video camera systems, video streaming applications, and remotely provided network services (ex. print services, directory services, file services).
5. Oracle Licenses: DoIT will not procure, maintain or renew Oracle licenses.
6. Agency's secure file transfer systems.
7. Agencies VoIP solutions that are not the Enterprise standard.

8. Non-enterprise agency server level administrative function on the operating system.
9. Provision or order network circuits needed to connect to the DoIT data center.
10. MSSQL, Oracle and other Database system Administration, vulnerability remediation and configuration.
11. Add resource capacity without prior request.

C. Optional Services

Auxiliary services may be available upon request from the Customer for an additional cost. These costs are not included in the budgeted services that DoIT provides and shall be the responsibility of the requesting agency. For any work requested in this area, DoIT will not be able to proceed until fully funded by the requester through a funds certification document and signed Statement of Work.

The following services are add-ons that may be requested. Costs for these items are variable and will be clearly defined and agreed to before moving forward with the request.

1. IT consultation during construction and operations to assist with application troubleshooting, tuning, or performance monitoring**.**

II. Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	● Established connectivity to Network Maryland (nwMaryland) ● Ability to provide information/documentation about existing infrastructure and supported dependent services. ● Acceptance of Managed Services agreement and standard SLAs ● Acquiring any needed assistance to on-board to the service or for assistance in using the service ● Payment for all service costs at the agreed interval, as published in the DoIT rate schedules ● Reporting any service-related issues to DoIT help desk
Technical:	● Customer Responsibility: Application installation, application layer security, application maintenance, and application support. ● Customer Responsibility: Design, develop, deploy, and test the database and maintain its interaction with application(s)

	• Customer Responsibility: Upgrade, patch, and remediate Oracle, MS SQL and other databases security vulnerabilities
Non-Technical:	• Client role definitions for escalation support • Provide 24 x 7 x 365 points of contact (3) for coordinating outages, emergency maintenance/restoration (with appropriate application access to provide technical assistance), and change management

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for Customer (Enterprise)
DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. Public Cloud Consulting Services
2. Well Architectured AWS Account
3. Cloud Governance & Security
4. Platform Hosting
5. Network: Connectivity to public cloud infrastructure
6. Operating System installation and Patching
7. Replication and regional Disaster Recovery solution
8. Capacity Monitoring and server performance tuning
9. FinOPS: Cost Optimization
10. VDI solution: Amazon Workspace
11. Engineering support: M-F, 8am - 5PM
12. Vendor Contract management with Reseller
13. Assist in reviewing reseller invoicing for public cloud services; upon requested
14. Okta iDP for AWS IAM Access
15. Technology Refresh

B. DoIT Responsibilities for Customer (Non-Enterprise)
DoIT shall be responsible for the following activities in coordination with the Customer for which DoIT does not provide enterprise managed services:

1. Public Cloud Consulting
2. NetworkMD: Connectivity to infrastructure on public cloud

3. Assist in reviewing reseller invoicing for public cloud services; upon requested
4. Well Architectured AWS Account
5. Okta iDP for AWS IAM Access

** Non-Enterprise agencies do not get monitoring services and DoIT does not have access to their AD.

C. Customer Entity Responsibilities

The Customer Entity shall be responsible for the following activities:

1. Provide additional scope/funding if application requirements are outside of the scope of a standard server build.
2. Configuration and maintenance of everything above or installed on the Server Operating System - Some examples include but are not limited to:
    a) Agency specific application in support of mission
    b) Applications required for agency operations
    c) COTS software
    d) COTS software required for use by or in conjunction with an application
    e) Services that are part of said services
    f) Web/database components that are used in association with a hosted application
3. Assume responsibility for use of services by any user who accesses the hosting services environment with the Client's account credentials.
4. Be responsible for obtaining all necessary permissions to use, provide, store and process content in the hosted environment and grant DoIT permission to do the same.
5. Install all database programs to suit their specifications. Native database backups are the responsibility of the customer.

IV. Service Level Agreements (SLA's)

A. Availability

Service availability includes the duration of time the service is operational during a [calendar month or twenty-four (24) hour period] and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	99.9% uptime
Capacity	
Reliability	100% (AWS Public Cloud)

B. Request Fulfillment Timeframe Service Level Objectives (SLOs)

1. AWS publishes SLO per Service see url for latest information see: https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/appendix-a-designed-for-availability-for-select-aws-services.html

Timeframe SLO Notes/Dependencies	**Timeframe SLO Notes/Dependencies**	**Timeframe SLO Notes/Dependencies**
Provisioning well Architected AWS Account	7 Calendar Days	Assumption: 1) All special Intake processes are completed. **Dependencies:** 1) Customers bring appropriate technical staff to design meetings scheduled 2) Customer submits accurate supplemental cases – e.g., admin access, firewall, Workorder signature 3) PO provided for funding source
Build/Refresh /Rebuild	3 Calendar Days	Assumption: 2) All special Intake processes are completed. 3) Based on “average” complexity case; 4 servers or less, only 1-2 design meetings required.
Decomm Service	5 Calendar days	Date from the requested decommission date in which the service is taken offline
Critical Vulnerability Patching	15 days	
Moderate Vulnerability Patching	60 days	

Low Vulnerability Patching	90 days	

C. Maintenance
DoIT may modify the service without degrading its functionality or security features.

1. Scheduled Maintenance
Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.
    a) Scheduled maintenance will be performed outside of normal business hours (7pm - 6am Monday - Friday)
    b) The customer will be notified no less than five (5) business days prior to the scheduled activity.
    c) Within twenty-four (24) hours after the completion of the scheduled activity, the Customer will be notified.

2. Unplanned Maintenance
    a) DoIT will attempt to notify the Customer of any unplanned maintenance activities no less than two (2) hours prior to commencement. Note: Emergency activities requiring immediate remediation may not allow ample time for notification.
    b) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the Customer will be notified.

D. Service Delivery
DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	**Measure**
Initial Ticket Response and Customer Contact	1 Business Day during normal hours for Incidents with priority 2-4
Other Areas	Please see **Request Fulfillment Timeframe Service Level Objectives (SLOs)**
Major Incident	Priority Incidents (P1), 15 minutes. This includes security breach, Infrastructure crash

V. Support and Service Management

A. Support

DoIT will provide support via telephone, email, or in-person according to the SLA's outlined above.

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support.
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support (Vendor) will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

Priority (P)	Description	Response Time	Resolution
P1	An incident that results in a total cessation of service across the Customer. Ex: Complete loss of service, the production system is down or inaccessible and the backup redundancy is also down.	[2] hours	[24] hours
P2	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions. Ex: Applies to both Production systems. The system is up and running, but a critical loss of application functionality or performance resulting in a high number of users unable to perform their normal activities. Inconvenient workaround or no workaround exists	[4] hours	[2] business days
P3	Disruption of service for of non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes	[2] business days	[5] business days
P4	A single user incident	[3] business days	[5] business days
P5			

*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.

Request Management

Requests to move, add, or change service shall be handled as follows:

1. New Service(s)
   Entities seeking to utilize the service or deploy optional services outlined herein must:
   a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
      - DoIT will evaluate the request to ensure that the service meets the entity's business needs.

2. Service Modifications
   To increase, decrease, or alter existing service, the Customer must:
   a) Submit a request via email to doit.intake@maryland.gov
      - Service modifications include increasing or decreasing quantity of units, adding new services, engineering consulting services.
      - DoIT will log the request and assign it to the appropriate team for fulfillment.
      - Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

C. Outages
   DoIT will notify the Customer via email of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions.

D. Support and Service Management Exclusions:
   While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

   1. Development, technical support or management of customer applications
   2. Repairs or services for the customer's third-party technologies.
   3. Spearheading Customer initiatives
   4. Project management
   5. Support for Non-Standard DoIT offering

VI. Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. The Customer charges budgeted for the current fiscal year are outlined in the DoIT Shared Services Annual Invoice.

1. The unit of measure for which charges are derived for this service is consumption based. Cloud Services Recommend:

2. Reference the current fiscal year Rate Sheet for additional information

B. All services delivered by DoIT under this agreement are done so on a 100% reimbursable model and therefore costs will be evaluated and adjusted annually to account for fluctuations in the number of shared services used and the underlying costs to deliver that service.

VII. Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. The customer must provide ninety (90) days advance written notice to terminate services. Due to the nature of the state financial system budgeting for IT services, terminations will only be effective at the end of the fiscal year following the conclusion of the ninety (90) day notice period.

VIII. Warranty, Limitations, and Exclusions

A. N/A