Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

SERVICE AGREEMENT

Between
The Maryland Department of Information Technology and
User Agency
For
Third-Party Compute & Storage Options (AWS)
(FY2021)

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

1 Services Covered

DoIT offers third-party compute 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 NetworkMD 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.

2 Parties Responsibilities

2.1 DoIT's Responsibilities:

DoIT shall provide:

- Assistance to the client with the development of work order. There are two types of work orders. One work orders covers an estimation of AWS utilization rates based on what is hosted in the Public Cloud Hosting platform. 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.
- Work order modifications if costs will exceed currently executed work orders.
- Account provisioning
- Deployment and configuration a standardized architecture for the Center for Internet Security (CIS) AWS Foundations Benchmark
- Enabling of cross-account access
- VPC Network Setup
- Classless Inter-Domain Routing (CIDR) IP address assignments from networkMaryland.
- Creation of subnets, routing tables, virtual firewalls (NACL/Security Group), endpoints, NAT, Internet, and Virtual Private Gateways.
- Hardening to CIS AWS Foundation standards.

- AWS IAM management consisting of setting up password policies, users, groups, roles and follow resource naming and tagging standards.
- Direct Connect setup to Configure public and private virtual interface and VPN configuration.
- Security Operations which include a centralized security log management, anti-virus and vulnerability assessment *
- Develop cost estimates for Public Hosting services.
- Account billing and cost alerting.
- Guidance on AWS best practices and design.
- Encryption for EBS volumes and S3 Buckets to be enabled upon request.
- Administration and Management of the Hosting Shared Services Web Application Firewall (WAF) include the following:
- FIPS certified web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication.
- Performs packet inspection of HTTP, HTTPS, and XML as well as protection against critical web application security risks.
- (OWASP) security threats.
- Protects against SQL injection attack; cross-site scripting attacks; cookie tampering; form validation and protection; HTTP and XML reply and request format validation; JSON payload inspection; signature and behavior based protections; data loss prevention (DLP) support, including the monitoring of traffic for intended and unintended data exposure; DoS protection; authentication, authorization, and auditing support and reporting; and policy tools that provide for easier PCI-DSS compliance verification.

2.2 DoIT shall not be responsible for the following under this Service Agreement:

- Firewall services that are not part of the web application firewall.
- Customer application support which includes but is not limited to web sites and applications, COTs software applications, databases, database administration, native database backup maintenance plans, application upgrades or customizations and database encryption. Any associated technologies, software applications, specialized software, custom configurations (ex: host files updates or user profile management on Servers) used in conjunction with an application, delivery or presentation of the application.
- DoIT does not provide virtual server hypervisor console access.
- An agency’s remote devices and services (i.e. any devices not hosted within MD DoIT’s private cloud environment/data center). Examples include; physical or virtual servers, scanning devices, storage devices, server backups, video camera systems, video streaming applications, and remotely provided network services (ex. print services, directory services, file services).
- DoIT will not procure, maintain or renew Oracle licenses.
- Agency secure file transfer systems.
- VoIP solutions that are not the Enterprise standard

2.3 User Agency's Responsibilities:

User Agency shall:

- Provide routing devices to connect to the Public Cloud Hosting environment.
- Order circuits to connect to the Public Cloud Hosting environment.
- Non-enterprise need to provide firewall and router configuration and associated administrative support.
- Develop the content of a professional contractual services work order.
- Work with DoIT Public Cloud Hosting Team to provide server specifications and other pertinent system details to develop a work order covering AWS utilization. (Examples: Server sizing, disaster recovery with regions or availability zones, storage capacity, data transactions, software licensing, backup storage capacity along with data retention policies, SSL certificates and other software licenses required for support of the project).
- Provide hardware and software specific for their hosted application to access and/or use in the Public Cloud Hosted platform. This will include any client specific URL address and associated certificates.
- Responsibility for SSL Certificate renewals and replacements. Purchases can be made through DoIT's SSL Enterprise subscription services.
- Create and managing EC2 instances
- Responsibility for ensuring hosting costs stay within what was budgeted for in the defined work order amounts. Change modifications can be made to a work order to increase the budgeted dollar amount
- Let Public Cloud Hosting Team know if EC2 encryption is required on a server instance.

3 Service Level Agreements

- Support Hours: 8AM - 5PM Monday - Friday
- Uptime: 99.9%
- Response time and resolution targets:
  - Priority 1 (P1) response time 2 hours, resolve time 4 hours
  - Priority 2 (P2) response time 4 hours, resolve time 2 days
  - Priority 3 (P3) response time 1 day, resolve time 3 days
  - Priority 4 & 5 (P4/P5) response time 2 days, resolve time 5 days
- Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.

4 Maintenance Schedules*

Windows updates and patches applied to servers the third week of every month Tuesday - Thursday from 7:00PM - 12:00AM. DoIT will provide notice to the User Agency at least 5 days in advance of any planned maintenance. DoIT will document a list of all weekly and monthly changes planned in order to limit disruption to the user agency's environment. DoIT may modify a Cloud Service, without degrading its functionality or security features. Any change that affects the commercial terms of the Cloud Services will not be effective until the next agreed renewal or extension. Changes to the hosting environment are not retroactive, they apply as of the effective date only to new orders or ongoing Cloud Services that do not expire and renewals.

Non-Enterprise Customers:

- Server patching, end-point protection (anti-virus), server monitoring are not available.

5 Support and Service Outages

Normal hours of operation for DoIT technical support staff are 8AM – 5PM Monday - Friday (excluding holidays).

6 Costs for Services

The cost of the covered services is outlined in DoIT's Cost Allocation Schedule, which is the DoIT Shared Services- Annual Invoice, for the current fiscal year.

7 Termination of Services

Agency must provide 60 days' advance written notice to terminate services.

* Represents Services provided to Enterprise customers only.