

## SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and  
the Customer

for

Cloud Services (Server & Storage, Co-location, Data Center)

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

Private Cloud Hosting is a shared, multi-tenant infrastructure service where IT services are provisioned over private IT hardware infrastructure hosted in the TierPoint Data Center, managed by DoIT IT staff, for a customer organization. The infrastructure can be leveraged by customer-to-host applications and services, upon request. Additionally, customers receive the benefit of the Server Management Service (SMS) bundle to leverage the technical expertise of DoIT’s technical engineering team. The enterprise-shared services bundle includes patch management, endpoint protection, network monitoring and a standardized network architecture.

#### A. Standard Service:

The following components are included with the standard service:

Standard Service Name	Service Type	Notes
Servers	2vCPU, 4GB RAM and 90G Drive	Agency can buy additional resources at cost
Operating System	Windows Server Operating System	N** (standard OS): v2022 N-1: v2019 N-2: v2016 All includes R2 as well
Operating System	RedHat	N (standard OS): v8

		N-1: v7
Operating System	Ubuntu	N (standard OS): v22 N-1: v20
Network Connectivity	1 IP Address	More can be requested. Standard is 1 IP address
Server Management Tools	Endpoint protection and monitoring	<ul style="list-style-type: none"> <li>- Tanium</li> <li>- CrowdStrike</li> <li>- Nessus scanning</li> <li>- ScienceLogic</li> </ul>
System Software Licenses	Server Operating Systems (OS)	<ol style="list-style-type: none"> <li>1) System software procurement</li> <li>2) Maintenance contract management</li> <li>3) Hardware procurement and maintenance</li> </ol>
Application Software Licenses	MS SQL	MS SQL Standard Software Assurance (Covers 2 cores, 4 core minimum required per server)
Patch Management	OS Monthly Patching	<a href="https://drive.google.com/file/d/1NdOCW-thmLWApqa0maNLX9tB_1B6HG1X/view">https://drive.google.com/file/d/1NdOCW-thmLWApqa0maNLX9tB_1B6HG1X/view</a>
Security Vulnerabilities	Remediation support	Server Operating System only for In-scope managed systems hosted out of TierPoint Data Center managed by DoIT
Load Balancing Services		Traffic Management
Remote Desktop Server Client Access	2 Licenses	Additional Terminal Server licenses at cost
Disaster Recovery	Part of the bundled services. Disaster Recovery consists of the planning and preparation necessary to recover critical information systems hosted on TierPoint Data Center	For in-scope enterprise agencies hosted out of TierPoint Data Center that DoIT manages.
IT Consulting Services		

Datacenter	TierPoint Data Center, co-location	certified in SSAE18 Type 2 SOC II, PCI-DSS, GLBA and HIPAA compliant
------------	---------------------------------------	--

**\*\*The current release version is known as N and the prior major version of the software as N-1. Older versions of software are labeled as N-2, N-3, etc.**

#### B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Customer application support includes but is not limited to websites and applications, databases, database administration, native database backup maintenance plans, COTs software applications, application upgrades or customizations and database encryption.
2. Access: DoIT will not provide console access to the virtual server or hypervisor console, customers will only have access to their virtual servers via the Remote Desktop Protocol (RDP) or Secure Shell access (SSH) methods.
3. 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).
4. Oracle Licenses: DoIT will not procure, maintain or renew Oracle licenses.
5. Agency's secure file transfer systems.
6. Nested virtualization technologies within a hosted virtual machine
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 Administration 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. Customers occasionally require additional support outside of normal business hours to accommodate installations, upgrades, or during critical processing time.
2. Consulting services early in a project's life cycle – during inception or assessment, discovery or later during alternative or procurement analysis.
3. 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:

<b>DoIT Services:</b>	<ul style="list-style-type: none"><li>• Established connectivity to Network Maryland (nwMaryland)</li><li>• Ability to provide information about existing infrastructure and services</li><li>• Acceptance of Managed Services agreement and standard SLAs</li><li>• Acquiring any needed assistance to on-board to the service or for assistance in using the service</li><li>• Payment for all service costs at the agreed interval, as published in the DoIT rate schedules</li><li>• Reporting any service-related issues to DoIT help desk</li></ul>
<b>Technical:</b>	<ul style="list-style-type: none"><li>• Customer Responsibility: Application installation, application layer security, application maintenance, and application support.</li><li>• Customer Responsibility: Design, develop, deploy, and test the database and maintain its interaction with application(s)</li><li>• Customer Responsibility: Upgrade, patch, and remediate Oracle, MS SQL and other databases security vulnerabilities</li></ul>
<b>Non-Technical:</b>	<ul style="list-style-type: none"><li>• Client role definitions for escalation</li><li>• 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</li></ul>

### 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 Enterprise Managed Customers

DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. Platform Hosting -Windows and Linux
2. Network: Connectivity to infrastructure
3. Load Balancing services
4. Operating System installation and Patching
5. Backup as a Service using Commvault
6. Disaster Recovery: consists of the planning and preparation necessary to recover critical information technology systems hosted in TierPoint Data center.
7. Server Monitoring (using ScienceLogic) and Service Desk support
8. Capacity Monitoring and server performance tuning
9. Software procurement and Assurance (Server OS)
10. Software Assurance (MS SQL database)
11. Hardware procurement and maintenance
12. Engineering support: M-F, 8am - 5PM
13. Vendor Contract management
14. Technology Refresh

#### B. DoIT Responsibilities for Non-Enterprise managed customers

DoIT shall be responsible for the following activities in coordination with the Customer for which DoIT does not provide enterprise managed services:

1. Platform Hosting -Windows and Linux
2. Network: Connectivity to infrastructure
3. Load Balancing services
4. Operating System installation (patching is not included)
5. Backup as a Service
6. Disaster Recovery: consists of the planning and preparation necessary to recover critical hosted system in the TierPoint Data center.
7. Capacity Monitoring and server performance tuning
8. Software procurement and Assurance (Server OS and MS SQL database)
9. Hardware procurement and maintenance
10. Engineering support: M-F, 8am - 5PM

## 11. Vendor Contract management

\*\* 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. Assume responsibility for security directly related to the 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	99.99% (Infrastructure Components (Power System, Racks))

### B. Windows Request Fulfillment Timeframe Service Level Objectives (SLOs)

Server Option Timeframe SLO Notes/Dependencies	Server Option Timeframe SLO Notes/Dependencies	Server Option Timeframe SLO Notes/Dependencies
Server Build/Refresh /Rebuild	2 Days	**Based on "average" complexity case; 4

		<p>servers or less, only 1-2 design meetings required.</p> <p>***This does NOT include customer application load and testing. That is not a DoIT responsibility.</p> <p><b>Dependencies:</b></p> <ul style="list-style-type: none"> <li>1) Customers bring appropriate technical staff to design meetings scheduled</li> <li>2) Customer submits accurate supplemental cases – e.g., admin access, firewall.</li> <li>3) Cases DoIT and Customer placed in "hold" status may delay completion.</li> <li>4) Assuming all Special Intake process was followed and approval/funding was secured</li> </ul>
Server Decommission	7 Calendar days	Date from the requested decommission date in which server is taken offline and infrastructure removed
Add Memory/Storage/Cores	1 Business Day	Additional Core requests require a reboot; if a customer needs reboot to be scheduled around its application M&O schedule this could result in delays beyond the 1-day turnaround.
Restore Files	1 Business Day	Applies to restoring Files and File Folders only; complete system restores will take longer
Add Monitoring	1 Business Day	Applies to "Standard"

		requests - using existing functionality within the DoIT monitoring application; custom requests that require additional configuration could take longer.
Admin/RDP Access	1 Business Day	May require additional time if the request is tied to a New Server Build/Refresh/Rebuild; relies on completion of server build.
Critical Vulnerability Patching	15 days for patching.  1 day for network segmentation	A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts.
Moderate Vulnerability Patching	60 days	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations
Low Vulnerability Patching	90 days	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component. Microsoft recommends that customers evaluate whether to apply the security update to the affected systems.



### 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 <b>Windows Request Fulfillment Timeframe Service Level Objectives (SLOs)</b>
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\*:

<b>Priority (P)</b>	<b>Description</b>	<b>Response Time</b>	<b>Resolution</b>
P1	An incident that results in a total cessation of service across the Customer. Critical issue that severely impacts the service. The situation halts business operations and no acceptable workaround exists. 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	Single user Impact	[2] business days	[5] business days

P5			
<p>*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.</p>			

## 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](mailto: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](mailto: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 offerings
6. Support of agency in-house Disaster Recovery plan

## 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 per device.
    - a) Windows/Linux Virtual Server: Annual cost/per server
    - b) Windows/Linux Virtual Operating System: Set-up Fee: one time setup cost/per server
    - c) Windows/Linux Enterprise Edition: License cost/per server
    - d) Additional Cores: per Core
    - e) Additional Memory: per GB
    - f) Additional RAM: per GB
    - g) Database License:
      - o MS SQL: per License
    - h) Server Monitoring Tool: Annual/per server
    - i) Additional Services: SoW based
  - 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

This section is not applicable