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

Customer

For

Network-Attached Storage 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

Private Cloud Hosting for network-attached storage (NAS) is a DoIT Cloud Services offering where Tier 1/2 NAS services (table 1) are provisioned atop private DoIT hardware infrastructure hosted in the TierPoint Data Center and is managed by DoIT IT staff for the customer organization. The infrastructure can be leveraged by customers to provide NAS services for individual users and agency business units. Additionally, customers receive the benefit of leveraging the technical expertise of DoIT's technical engineering team to provide component hardware and software upgrades, resource monitoring, a standardized network architecture and hardware lifecycle planning.

A. Standard Service:

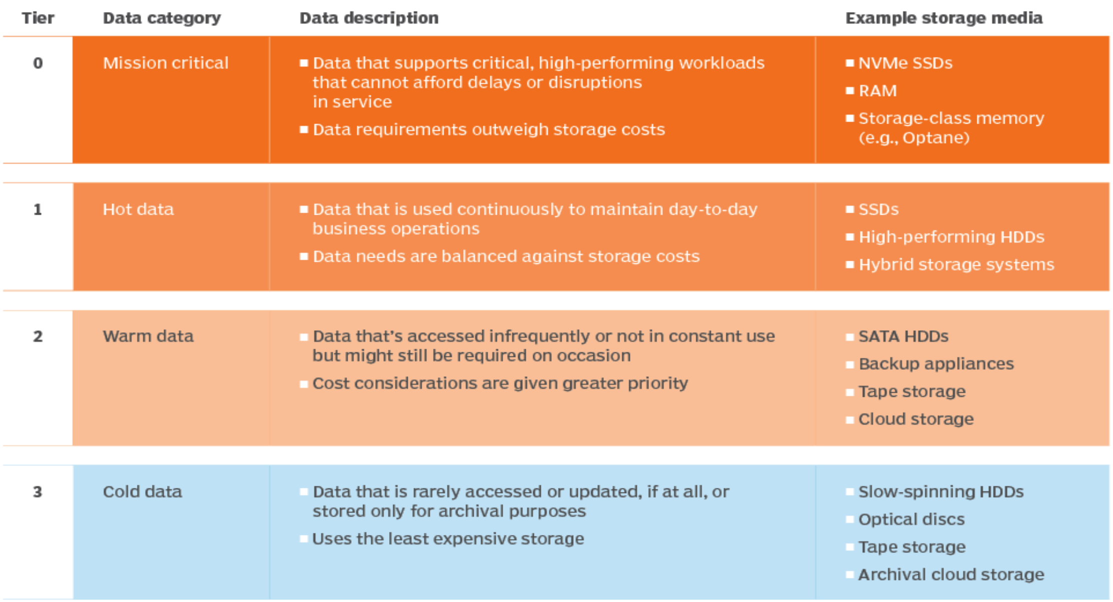
The following components are included with the standard service:

- A dedicated storage destination for hosting an agency's network file systems (ex. User home directories, departmental shared drives)
- Protocols supported include both CIFS/SMB and NFS protocols
- Granular security for file systems and directories
- End-user access to snapshots for data retrieval
- 30-day retention of files and directories (with the exception of 7-days for the retention of native SQL backup files)
- Off-site replication to a secondary data center

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Tier 0 (**table 1**) storage performance requirements (ex. high-performance workloads)
2. Tier 3 (**table 1**) storage performance requirements (ex. data archival workloads)
3. Application-specific use cases with high storage capacity requirements (ex. electronic document repositories, video archiving)
4. Agency's remote NAS devices and services (i.e., any devices not hosted within MD DoIT's private cloud environment/data center).
    a) Examples include NAS hardware devices, physical or virtual file servers
5. Non-enterprise agency administrative function within the file system
6. Implementation of Windows Distributed File System (DFS)
7. Provision or order network circuits needed to connect to the DoIT data center.
8. Adding resource capacity without prior request.



Tier	Data category	Data description	Example storage media
0	Mission critical	■ Data that supports critical, high-performing workloads that cannot afford delays or disruptions in service ■ Data requirements outweigh storage costs	■ NVMe SSDs ■ RAM ■ Storage-class memory (e.g., Optane)
1	Hot data	■ Data that is used continuously to maintain day-to-day business operations ■ Data needs are balanced against storage costs	■ SSDs ■ High-performing HDDs ■ Hybrid storage systems
2	Warm data	■ Data that's accessed infrequently or not in constant use but might still be required on occasion ■ Cost considerations are given greater priority	■ SATA HDDs ■ Backup appliances ■ Tape storage ■ Cloud storage
3	Cold data	■ Data that is rarely accessed or updated, if at all, or stored only for archival purposes ■ Uses the least expensive storage	■ Slow-spinning HDDs ■ Optical discs ■ Tape storage ■ Archival cloud storage

Table 1: Data Storage Tiering Hierarchy

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.

1. Tier 0 (table 1) storage performance requirements
    a) High-performance workloads
2. Tier 3 (table 1) storage performance requirements
    a) Data archival workloads

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:	● Ability to provide information about existing infrastructure and services ● Acceptance of Managed Services agreement, which includes 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:	● The ability to create or leverage a lightweight directory access platform (ex. LDAP, Microsoft Active Directory) and DNS services*
Non-Technical:	● Client role definitions for escalation ● 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.

* Non-Enterprise agencies do not receive assistance configuring granular security permissions, DNS configurations, or DFS technologies as DoIT staff does not have access to their Active Directory instances.

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. Multi-tenant NAS storage platform
2. Network connectivity to NAS infrastructure
3. Platform hardware and software upgrades
4. Performance monitoring

5. File system backups with 30-day retention
6. Off-site replication of file system datasets
7. Technical Engineering support: M-F, 8AM - 5PM
8. Vendor contract management
9. Hardware lifecycle planning

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. Multi-tenant NAS storage platform
2. Network connectivity to NAS infrastructure
3. Platform hardware and software upgrades
4. Performance monitoring
5. File system backups with 30-day retention
6. Off-site replication of file system datasets
7. Technical Engineering support: M-F, 8AM - 5PM
8. Vendor contract management
9. Hardware lifecycle planning

C. Customer Entity Responsibilities

The Customer Entity shall be responsible for the following activities:

1. Provide additional scope/funding if file services requirements are outside the scope of a standard network-attached storage use case.
2. Assume overall responsibility for identifying which users and groups obtain file and directory access along with the level of access
3. Assume responsibility for use of services by any user who accesses the hosting services environment with the client's account credentials.
4. Non-Enterprise customers do not receive assistance configuring granular security permissions, DNS configurations, or DFS technologies as DoIT staff does not have access to their Active Directory instances.

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. Request Fulfillment Timeframe Service Level Objectives (SLOs)

Timeframe SLO Notes/Dependencies	Timeframe SLO Notes/Dependencies	Timeframe SLO Notes/Dependencies
Agency Storage Virtual Machine (SVM) provisioning	1 Day	Assuming its a greenfield build and it has gone through the special intake requests with all approvals
Network Attached Storage Decommission	7 Calendar days	Date from the requested decommission date in which the volume/SVM is taken offline and resources removed
Add Storage	1 Business Day	
Critical Vulnerability Patching	15 days	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.

Cyber Incident Recovery SLA/RTO

Scenario	Scope of Failure	Business Impact	Time to Recover Today (RTO)
Deleted or Corrupted Small Size File (<5MB)	1 file	Low	Variable based on file-count: Average 30 minutes
Deleted or Corrupted Medium Size File (50MB)	1 file	Low	Variable based on file-count: Average 30 minutes
Deleted or Corrupted Large Size File (5GB)	1 file	Low	Variable based on file-count: Average 30 minutes
Production NAS Storage Array Corruption	All Agency NAS Data	High	24 hours
Production and DR NAS Storage Array Corruption	All Agency NAS Data	High	Feature not available, 100% data loss, not recoverable
Large-Scale Malware Attack on NAS Data	All or Individual Agency NAS Data SVMs	High	100% data loss, not recoverable

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 2-3
Other Areas	Please see **Request Fulfillment Timeframe Service Level Objectives and Cyber File Recovery SLO/RTO section**
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	Description	Response	Resolution

(P)		Time	
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			
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 (managing customer NAS)

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
      a) Per GB/per agency/annually
   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