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

Disaster Recovery as a Service (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

In today's digital-centric landscape, organizations depend on infrastructure, applications, and data that are up and running 24/7. The combination of downtime and data loss can render an agency offline, make critical public services unavailable, and even threaten statewide security. Disasters that cause IT downtime and data loss range in size and scope from local cyber attacks to regional natural disasters. Thorough security and organizational resilience strategies are crucial for agencies looking to remain available, thrive, and face these threats to their digital assets.

Disaster Recovery as a Service (DRaaS) allows disaster recovery operations to occur in a hosted cloud environment in a geographically dispersed region of the United States. With DRaaS, DoIT will mirror on-premises systems to the regionally diverse environment and create secure connectivity between them. This will provide redundancy should the primary data center go offline, providing the ability to switch applications to mirrored copies and reinitialize them to support ongoing organizational operations. Implementing DRaaS can help state agencies ensure they are prepared for any disruptions, providing peace of mind and maintaining public trust.

A. Standard Service:

1. Data Replication: DRaaS relies on continuous data replication to create real-time copies of critical data and applications. This ensures that in the event of a disaster, agencies can switch to the replicated data, minimizing data loss and downtime. The hosted agency's virtual machine (VM) and network-attached storage (NAS) data sets will be replicated.

2. Failover and Failback: Should DoIT's primary data center experience a catastrophic failure rendering it unusable, an agency's digital assets will be recovered and made usable at the DR site. One of the key advantages of DRaaS is its ability to orchestrate the failover and failback processes for higher-level components in the infrastructure stack (e.g. virtual machines).

3. Scalability: The DRaaS solution is designed as a flexible and scalable platform to accommodate changes such as the expansion of an agency's digital assets or a fluctuation in the volume of agency data.

4. Testing and Verification: DoIT will conduct annual DR tests allowing us to identify and address potential issues before a real disaster strikes.

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Customer application support once a virtual machine or network-attached file system (NAS) has been recovered. This includes but is not limited to websites and applications, databases, database administration, native database backup maintenance plans, COTs software applications, application licensing requirements, and application upgrades or customizations and database encryption. Applications remain the customer's responsibility.

2. Access: DoIT will not provide access to the software and hardware mechanisms providing replication and recovery operations

3. Access: DoIT will not provide console access to the virtual server or hypervisor consoles of the recovery environment, customers will only have access to their recovered virtual servers via the Remote Desktop Protocol (RDP) or Secure Shell access (SSH) methods.

4. 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, hypervisors, scanning devices, storage devices, server backup system, video camera systems, video streaming applications, and remotely provided network services (e.g. print services, directory services, file services).

5. Individual agency failover requests if the primary data center is online and functional (note; this does not include failover testing).

6. Administrative functions related to the operating system of a recovered virtual machine for non-enterprise agency servers.

7. MSSQL, Oracle and other Database Administration and configuration of the DBMS on a recovered virtual machine.

8. This service replicates existing infrastructure and is not a method to change that service. Requests for service changes must come through the standard DoIT intake process to make changes to the primary hosted environments that will then be mirrored under this offering.

9. Additional scope/funding if application recovery requirements are outside of the scope of a standard recovery

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.

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 • Digital resources must be hosted within MD DoIT's private cloud environment/data center (e.g. virtual machines, NAS file systems) • Subscriber of DoIT's Managed Firewall Service • Ability to provide information about existing applications, infrastructure and 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, application recovery and application support. • Customer Responsibility: Design, develop, deploy, and test the

	database and maintain its recoverability from a crash-consistent copy ● Customer Responsibility: Upgrade, patch, and remediate Oracle, MS SQL and other databases security vulnerabilities which could affect recoverability
Non-Technical:	● Client role definitions for escalation ● Provide 24 x 7 x 365 points of contact (1) 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 Enterprise Managed Customers and Non-Enterprise Managed Customers

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

1. Planning and preparation operations necessary to recover critical information technology systems hosted in TierPoint Data center.
2. Recover agency virtual machines at the DR site
3. Recover agency network-attached storage systems at the DR site
4. Establish nwMD network connectivity to digital assets at the DR site
5. Configure managed firewall services at the DR site
6. Setup backup operations at the DR site for recovered virtual machines
7. Failback virtual machines, NAS data sets, network connectivity, and firewall services to the production environment at the conclusion of a disaster event
8. Vendor Contract management for DRaaS
9. Technology refresh of DR environment
10. Test the DR environment annually

B. Customer Entity Responsibilities

The Customer shall be responsible for the following activities:

1. Provide a listing of all current critical applications and their associated resources to be included in an orchestrated application recovery group, and notification when new application stacks are deployed
2. Furnish a list of all application dependencies and resources which must also be included in an orchestrated application recovery group
3. Make agency staff available to perform application recovery and testing once a virtual machine has been recovered from a crash-consistent copy
4. Assume responsibility for security directly related to the application.
5. Assume responsibility for use of services by any user who accesses the hosting services environment with the Client's account credentials.
6. Be responsible for obtaining all necessary permissions to use, provide, store and process content in the recovered environment and grant DoIT permission to do the same.
7. Install all database programs to suit their specifications and provide recovery from a crash-consistent copy. Native database backups and recovery from them 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 and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	99.9% uptime
Capacity	100%
Reliability	99.99% (DR Infrastructure Components and Replication Mechanisms)

B. Tiered Recovery Approach

The tiered recovery approach shown in the table below categorizes IT assets and outlines RTO and RPO goals, their descriptions and functions, and the methods used for data replication and recovery (e.g. orchestrated or manual). RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are two metrics used to determine how quickly systems can be restored and how much data can be tolerated as lost following a

disruption. RTO is defined as the maximum acceptable downtime, while RPO defines the maximum acceptable data loss, measured in time.

Tier	Class	RTO	RPO	Description	Functions	Active/Warm (Prod/DR)	Data Replication
0	Core Services	<1 hour	=<5 mins	Base Infrastructure and common services to be restored prior to business functions	Network services (ex. Routers and Firewall, EDL servers), Servers, OS, dB, DNS, AD	Active/Warm (Prod/DR) automated and/or orchestrated failover	Near synchronous data replication - hypervisor-based replication -and-array based (NAS)
1	Public Safety Services	<4 hours	=<1 hour	Agencies with the greatest impact on public safety - requires immediate recovery	Public safety; Emergency responders and coordinators	Active/Warm (Prod/DR) orchestrated recovery	Near synchronous data replication - hypervisor-based replication -and-array based (NAS)
2	Managed Agencies and Services	48 hours	=<1 hour	May not meet the criteria of public safety, but will need to be brought up soon after	Less-impactful functions and agency services	Active/Warm (Prod/DR) orchestrated recovery	Near synchronous data replication - hypervisor-based replication -and-array based (NAS)

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) The components comprising the DRaaS solution are not user-facing; therefore, maintenance activities will be performed during normal business hours or after hours as needed.

2. Unplanned Maintenance

a) Users will be notified post-event of unplanned maintenance activities adversely affecting RPOs.

D. Disaster Recovery Service Delivery, Management, and Support

DoIT will deliver, manage, and support this service to the customer in a timely manner according to the following standards:

Department of Information Technology Disaster Recovery Plan

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.

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

F. 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

V. 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. All costs for this service are included in the private cloud hosting charges and will not incur additional costs under this agreement.

VI. Termination of Service

A. Because this service is entirely inclusive in the costs of hosted servers in the DoIT provided private cloud, agencies cannot terminate this service. It will be terminated automatically for any servers removed from private cloud hosting.

VII. Warranty, Limitations, and Exclusions

This section is not applicable