SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

The Customer

Backup-as-a-Service (BaaS)

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 provides integrated backup, recovery, and disaster recovery as part of the Backup-as-a-Service (BaaS) for DoIT hosted services. The BaaS system is in a shared hosting environment and is available to agencies to which DoIT provides managed services, full stack from LAN to Desktop to on-prem infrastructure support ("Enterprise Customer")

A.

B. Standard Service:

The following components are included with the standard service:

1. Backup and Restoration
    a) Virtual server backups are VMware vCenter based system backups only
        - The vCenter backups allow for restoration of an entire virtual server, virtual disk(s) and granular restoration of an individual file(s) or folder(s) on the server. This backup captures all files on the server including any database files. It allows for recovery of the individual database files (these are not native transactional database backups but flat file backups of the database files).
2. Physical server backups
    a) Full server restorations require the reinstallation of the operating system and backup agent to restore the server.
3. Add and remove servers to the backup architecture as provisioned and decommissioned.
4. Established backup schedule policies

a) Daily incremental backups.
b) Weekly full backups.
c) Custom backup schedules are available upon request. Such requests are approved on a case-by-case basis and will incur additional service fees.

5. Provide tiered approach to backup, including
    a) Primary copy which holds the most recent backup data sets (30 to 90 days) will be in Baltimore Datacenter. Storage for the first 30 days is on PURE technology which provides immutability protections for data integrity.
    b) Secondary copy of the primary data will be replicated to the BWI datacenter. No change in retention period.
    c) A third backup copy, which will provide immutability protection and safeguarding against regional disasters for 100% of the backup data, will be stored at Amazon's US-East-2 region (Ohio) in an Amazon S3 Glacier storage bucket. No change in data retention period.
6. Security
    a) Secure tenant isolation
    b) Ability to encrypt data at rest or in transit
    c) Backup set immutability

C. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Database and application backups and troubleshooting.
2. Oracle/SQL Database administration.
3. Recovery Time and Recovery Point Objectives (RTO/RPO) for restoration of database servers.
4. Establishment of connectivity to external servers not in DoIT datacenters.
5. Restoration of servers, files and folders in data centers not hosted in the DoIT private cloud data center.

D. 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.

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. 90 Days and beyond Data Retention request
    a) DoIT provides support to agencies subscribing to the Off-Premises storage solutions
    b) This can only be procured via:
        - Vendor: Amazon Web Services (AWS)
        - Service Type: Multiple Storage options based on scope
        - Reseller: Strategic Communications
        - Executed Contract: NASPO
        - Rate: Standard Instance Type, based on consumption
2. Salesforce Backups
    a) Enhanced data protection of the Salesforce environment
        - Exports of all objects
        - Recovery
    b) 30-day data retention

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 DoITs 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 databases 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 • 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. Backup and Restoration
2. Physical server backups
3. Add and remove servers to the backup architecture as provisioned and decommissioned.
4. Follow established backup schedule policies
    a) Daily incremental backups.
    b) Weekly full backs.
    c) Custom backup schedules are available upon request. Such requests are approved on a case-by-case basis and will incur additional service fees.
5. Perform monthly restore testing on random servers in the DoIT data center. This includes testing full virtual machines, files and folder trees.
    a) Test and restoration of data upon request from the agency via a Service Desk ticket to the Server and Storage workgroup.
6. Maintain the access, security, patching, vendor management and the ownership of the backup Infrastructure in DoIT datacenters.
7. Adhere to DoIT's approved/established Change Management process.
8. Provide daily engineering support: Continuous error monitoring and troubleshooting of issues/bugs.
    a) Review daily backup reports.
    b) Customer backup reports can be delivered to email upon request and are encouraged for daily agency review.
9. Provide Disaster Recovery (DR) support
    a) DoIT will restore VMs to infrastructure once it is available following a disaster.
    b) Restoration of service will be prioritized according to the overall statewide criticality with a focus on public safety and citizen engagement.

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

1. Backup and Restoration
2. Physical server backups

3. Add and remove servers to the backup architecture as provisioned and decommissioned.
4. Follow established backup schedule policies
5. Daily incremental backups.
6. Weekly full backs.
7. Custom backup schedules are available upon request. Such requests are approved on a case-by-case basis and will incur additional service fees.
8. Perform monthly restore testing on random servers in the DoIT data center. This includes testing full virtual machines, files and folder trees.
9. Test and restoration of data upon request from the agency via a Service Desk ticket to the Server and Storage workgroup.
10. Maintain the access, security, patching, vendor management and the ownership of the backup Infrastructure in DoIT datacenters.
11. Adhere to DoIT's approved/established Change Management process.
12. Provide daily engineering support: Continuous error monitoring and troubleshooting of issues/bugs.
13. Review daily backup reports.
14. Customer backup reports can be delivered to email upon request and are encouraged for daily agency review.
15. Provide Disaster Recovery (DR) support: Disaster Recovery consists of the planning and preparation necessary to recover backup data to assist with the restoration process
16. DoIT will restore VMs to infrastructure once it is available following a disaster.
17. Restoration of service will be prioritized according to the overall statewide criticality with a focus on public safety and citizen engagement.

C. Customer Responsibilities

The Customer shall be responsible for the following activities:

1. Work with DoIT and define a data restoration plan
    a) Create a tiered approach model that clearly states which server/application will be restored 1st, 2nd & 3rd based on its criticality and mission to business.
2. Notify DoIT through a Service Desk ticket when servers are decommissioned.
3. Native database backups and restorations are the responsibility of the agency to a network storage location or DoIT managed NAS. Database administrators can use the database backup copy to restore the database to its operational state along with its data and logs.
4. When applicable, provide local or domain access where backup service accounts are required.
5. Provide and maintain connectivity to remote locations outside of DoIT datacenters.

6. Monitor backup reports to verify server lists are current.
7. Assist with the restoration of virtual servers, files and folders upon DoIT request.
8. For extended retention periods, beyond 90 days, submit a Special Intake request. This may include additional funding paid by the agency.
9. Agencies are responsible for their own Disaster Recovery Plan and Continuity of Operations Plan (COOP).
10. Agencies application owners are responsible for managing, maintaining, and troubleshooting their applications.

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
Reliability	99.9% (Infrastructure Components (Power System, Racks))
Availability	99.9% uptime

B. Backup-as-a-Service SLA (Time to Recover)

Scope	Business Impact	Severity	Immutability Level	Time to Recover
1 Virtual Machines(VM)	Low	P4	Primary and AWS Copy	15 min
10VM	Low	P3	Primary and AWS Copy	1 hr
100 VMs	Medium	P1	Primary and AWS Copy	16 hr
250 VMs	High	P1	Primary and AWS Copy	40 hrs

C. Test and Restore SLA

Monthly	50 VMs, 100% success rate
Quarterly	All supported Enterprise agencies, 100% success rate

D. 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 (7 pm - 6 am 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.

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

Feature	**Datacenter (Baltimore)**	**Datacenter (BWI)**	**Off-Prem (AWS)**
Managed Service	Y	Y	Y
Offsite Backup Copy	Primary	Secondary	3rd Copy
Encrypt, Compress, Reduce	100%	100%	100%
VM Disk/ Volume Protection	100%	100%	100%
File/ Folder Protection	100%	100%	100%
Data Retention Cycle (Frequency/Retain)	30-90 Days	30-90 Days	90 days and beyond
Audit Support	Y	Y	Y
SLA Support	Y	Y	Y

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 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	Single User Incident	[2] business days	[5] business days
P5			
*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.			

C. 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, relocation of service.
        - 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.

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

E. 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 or management of customer applications
2. Repairs or services for the customer's third-party technologies.
3. Spearheading Customer initiatives
4. Support for Non-Standard Backup offering
5. 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 GB of protected data.
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