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

Multi-Factor Authentication (MFA)

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

The DoIT Multi-Factor Authentication team is responsible for the management & support of the login.md.gov tenant powered by Okta. This tenant manages the synchronization of user identity for authentication to cloud-based & on-premises applications that require multiple factors for authentication.

A. Standard Service:

The following components are included with the standard service:

1. Configuration of AD Agent to sync with the customer agency's domain controllers for account provisioning & deprovisioning..
2. Provisioning of access for birthright applications per the customer agency's needs. Birthright applications are common tools the new user will need on the first day of work with the user agency (mail, office, authentication, etc.).
3. Support for the following multi-factor methods:
    a) Use of Yubikey or WebAuthn hardware tokens
    b) Use of Okta Verify application on mobile devices or government provided workstations
    c) Use of Google Authenticator
    d) Use of Mobile Phone for delivery of verification code via SMS text or phone call.*
    e) Use of landline phone for delivery of audio verification code via phone call.*
    *The use of telephone authentication is projected to be removed at a future date.

4. Support for implementing Adaptive Multi-factor Authentication based on various criteria (i.e. location or network, reputation, limiting MFA options based on application)
5. DoIT support for management of multifactor options for customer agency's users.
6. Support for integration of the login.md.gov platform to support agency applications supporting the following protocols:
    a) SAML 2.0
    b) OIDC
    c) RADIUS
    d) WS-Federation

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Procurement or replacement of Yubikey or Webauthn hardware tokens
2. Funding of application modification, licensing or update for support for MFA through login.md.gov.
3. Application management for integrations involving non-DoIT applications.

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.

.

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. Advanced Server Access - Support for implementing MFA login when admins login to servers. Support for SSH as well as RDP.
2. API Access Management

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:	• Synchronization of customer active directory users & groups. • Requires 2 servers on the agency active directory for the sync

	OR • Agreement for agency to be hosted.
Technical:	• Active Directory Functional Level minimum functional level of 2003. • .NET 4.6.2 or later on servers. • Minimum of TLS 1.2 support. • *2 AD Member Servers to run the Active Directory agent (for redundancy)* • AD Password Policy minimum based on the DoIT Security Manual.
Non-Technical:	• Provide 24 x 7 x 365 points of contact (3) for coordinating outages, emergency maintenance/restoration, 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. DoIT IAM Team will provision accounts from requests received from approved agency representatives.
2. DoIT Okta team will ensure accounts are provisioned with multifactor authentication.
3. DoIT IAM & Okta teams will ensure timely offboarding of active directory accounts and Okta accounts.
4. DoIT IAM & Okta teams will assist with providing support for transitioning access for offboarded personnel to other agency teams as requested.
5. DoIT Okta team will onboard agency applications as requested with Agency application admins support.

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. DoIT Okta Admins will provision access for Agency IT Account admins to manage MFA for said agency.
2. DoIT Okta Admins will support onboarding of applications for SSO into the login.md.gov platform on request through DoIT Intake.

C. Customer Responsibilities

The customer shall be responsible for the following activities:

1. Non-enterprise - Customer Agency IT AD Admins are responsible for onboarding and offboarding of users.
2. Enterprise - Customer Agency designated personnel.are expected to submit timely requests for user onboarding to DoIT via ServiceNOW onboarding requests.
3. Customer Agency designated personnel will inform DoIT IAM via ServiceNOW offboarding requests in a timely manner.
4. Customer Agency designated personnel.are expected to submit timely requests for user onboarding to DoIT via ServiceNOW onboarding requests.
5. Users will be onboarded and offboarded from Workday in a timely manner.
6. Customer Agency users needing assistance with login or MFA update will submit ServiceNOW incident ticket to receive assistance.
7. Customer Agency users will submit requests for integration of applications with login.md.gov via ServiceNOW request tickets.
8. Non-enterprise Customer Agency IT AD Admins are responsible for onboarding and offboarding of users.
9. Non-enterprise Agency Customer IT AD Admin team to manage their users' MFA information.
10. Non-enterprise agency AD IT Admins are responsible for notifying DoIT MFA team of issues via ServiceNOW incident tickets.
11. Non-enterprise agency AD IT Admins are responsible for notifying DoIT MFA team for integration of applications with login.md.gov via ServiceNOW request tickets to DoIT Intake.

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	Up to [1Gb] Varies by customer's location and equipment
Response Time	2 business days

B. 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 (8 pm - 6 am Monday - Friday; weekends and holidays)
   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.

C. 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	24 hours
Other Areas	
Other Areas	

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	Target Resolution
P1	An incident that results in a total cessation of service across the customer	[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.	[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
*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 (users)
        - 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. Project management

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 user.

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. Note that because multi factor authentication is a requirement for a number of additional services, canceling this will cause other services to no longer function.

VIII. Warranty, Limitations, and Exclusions

A. N/A