SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

The Customer

For

Secure Socket Layer (SSL) Certificate Management

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 SSL Certificate Management service is a DoIT Infrastructure security service that enables agencies to implement SSL certificates on servers facing the internet or general public. DoIT Infrastructure manages the configuration of the certificate management platform, management of certificate renewal, and certificate delivery while the customer is responsible for identifying their certificate needs.

A. Standard Service:
The Department of Information Technology (DoIT) shall provide the following standard service:
1. SSL certificate issuance
2. Domain validation for certificates
3. Certificate allocation reports
4. Platform Administration and Support
5. Subject alternate name consolidation
6. Vendor Support

B. Service Exclusions:
The following elements are excluded from the standard service offering:

1. Certificate subjects not facing the general public or internet.
2. Certificate Subjects where one of the following is not true:
    a) The server is managed through the State Content Delivery Network (CDN)
    b) The certificate subject is not using the State Domain Name Service (DNS) Management service.

3. Certificates needing extended validation exceeding normal validation done at the domain level.

C. Optional Services

Optional Services are available upon request from the customer at no additional cost. These services are included in the budgeted services that DoIT provides the requesting agency. Customers may request these services though a standard Intake ticket to doit.intake@maryland.gov

1. Access to a read-only account within the SSL Certificate Management platform to monitor certificates and assist the customer with identifying current and future needs.

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:	● Either State CDN or DNS Management ● DoIT Service Desk ● Maryland Security Operations Center (MDSOC)
Technical:	● Access to the certificate management platform is a Software-as-a-Service (SaaS) solution that requires access to the internet and ability to utilize multi-factor authentication.
Non-Technical:	● Customer must notify the Department of Information Technology Infrastructure (DoIT Infrastructure) of the Agency's SSL certificate needs. ● Customer must identify the Agency points of contact for this service. ● Customer must provide the DoIT/Infrastructure Administrators with up-to-date agency points of contact information (Additions/Deletions/Changes)

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities of 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 the customer

DoIT Infrastructure shall be responsible for the following activities in coordination with the customer receiving DoIT Security Awareness Training services:

1. Provide full administration of the SSL platform

2. Configure automated renewals and ensure certificates are in use on State CDN
3. Grant read-only access to the certificate management system as requested
4. Provide the customer with SSL consumption reports
5. Provide vendor contract management
6. Maintain and monitor SSL certificate consumption
7. Serve as the escalation point for SSL issues
8. Provide SSL certificate support
9. Optimize SSL subject alternate names to reduce costs to the state

B. Customer Responsibilities

The customer shall be responsible for the following activities:

1. Identify SSL certificate needs
2. Maintain a point of contact able to address SSL renewal and usage
3. Submit support tickets to the DoIT Service Desk with any identified issues

IV. Service Level Agreements (SLAs)

A. Availability

The Department of Information Technology SSL certificate solution is part of a Software as a Service (SaaS) offering. The SSL certificate availability is largely dependent on the SaaS vendor.

Service availability includes the duration of time the service is operational during a calendar year and the level at which the service functions. The table below further outlines the Department of Information Technology Infrastructure service targets with the SaaS vendor.

Category	Measure
Availability	SSL certificate solution availability target is 99.999% for 24x7x365

	• DoIT Infrastructure standard support: M-F, 8 am - 5 pm, excluding state-approved holidays • MDSOC incident support: 24x7x365

B. Maintenance

Scheduled Maintenance

The SSL solution SaaS vendor is responsible for performing and maintaining availability and reliability standards to include 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, 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.

Unplanned Maintenance

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.

a) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the customer will be notified.

C. Service Delivery

DoIT/Infrastructure SSL Certificate Administrators will deliver the requested services to the customer in a timely manner according to the following standards.

Category	**Measure**
Normal Changes	Normal changes will be assigned to a SSL certificate administrator within 1 business day of being assigned to the Infrastructure Service Now assignment group
Emergency Changes	Emergency changes will be assigned to a SSL certificate administrator immediately after being assigned to the Infrastructure Service Now assignment group

V. Support and Service Management

A. Support

DoIT will provide support via telephone, email, or in-person according to the SLAs 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 through 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
Priority 1:Critical Impact 1: Critical Urgency 1: High	An incident that results in a total cessation of service across the customer. Involves the loss of a critical business service or function ● The impact is statewide or affecting a public-facing/revenue-generating service on a widespread level. ● Multiple public safety and critical citizen systems/applications are impacted ● The disruption could result in regulatory, security, or reputational impact	2 Hours	24 hours
Priority 2: High Impact 2: High Urgency 1: High	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions. An issue is affecting a business component that isn't critical but is resulting in a disruption of the business service. Users are unable to perform normal business operations, and a workaround is not available. ● The issue can impact multiple agencies or a subset of multiple users ● The issue is affecting a high-level Executive.	4 hours	2 business days

Priority 3: Moderate Impact 3: Normal Urgency 1: High	Disruption of service of non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes. The impact causes a work stoppage for a single user - a workaround is not available ● A single user is not able to complete a time-sensitive critical task ● The user is marked as a VIP	2 business days	5 business days
Priority 4: Normal Impact 3: Normal Urgency 2: Medium	Minimal impact on business operations and can be resolved without significant disruption. A minor cosmetic issue on a non-critical webpage could be an example. ● An incident has impaired the user's ability to perform their normal business operations but a workaround is available ● An issue is affecting a single user that is not business critical or time-sensitive	4 business days	7 business days

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 the quantity of employee/contingent worker accounts.
      - DoIT will log the request and assign it to the appropriate team for fulfillment.

- Requests that involve increases in 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. All services delivered by DoIT under this agreement will be supported via OSM-appropriated funds unless identified consumption or specific requirements demand additional costs to support. Any further charges will be coordinated with the customer and signed off on before implementation.

VII. Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. Due to the nature of the managed service and its alignment with the Statewide Cybersecurity Centralization Strategy, non-exempt state agencies must obtain External SSL services from DoIT for official Maryland business requirements and therefore may not withdraw from the overall offering.

VIII. Warranty, Limitations, and Exclusions

A. N/A