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

Security Awareness Training (SAT)

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 Security Awareness Training service is a DoIT service that teaches employees how to protect their organization's assets and data, and cultivates a culture of cybersecurity by providing the customer with engaging microlearning content and phishing simulations to test the effectiveness of the training. The DoIT security awareness team manages the configuration of the training platform and the enrollment of agency users in training while the customer is responsible for providing the security awareness team with an accurate list of agency users.

A. Standard Service:
The Department of Information Technology (DoIT) shall provide the following standard service:

1. Security Awareness Training
2. Learner Assessments
3. Security Awareness Training Progress Reports
4. Platform Administration and Support
5. License Management
6. DoIT OSM SAT Support Team
7. Vendor Support

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

1. Any customizations not covered by the current contract.
2. On-site training.

3. Corrections to user template submissions submitted by Agency Security Awareness Managers to include the following:
    a) Employee First Name
    b) Employee Last Name
    c) Employee Email Address

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. Phishing simulations: Phishing simulations are imitations of real-world phishing emails departments can send to employees to test online behavior and assess knowledge levels regarding phishing attacks. The emails mirror cyber threats State of MD employees may encounter in their daily activities, both during and outside work hours.
2. Role-based Security Awareness Training: Comprehensive training covering management, operational, and technical roles and responsibilities. This includes physical, personnel, and technical safeguards and countermeasures. The training can also include policies, tools, and artifacts for the organizational roles defined.

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:	● Maryland.gov email account is required for access ● DoIT Service Desk ● Maryland Security Operations Center (MDSOC)
Technical:	● The security awareness training platform is a Software as a Service (SaaS) platform accessible to all authorized users with a compatible web browser and stable connection to the Internet. ● (Optional) Integration of customer identity provider (e.g., Okta, Active Directory, Azure) with the security awareness training platform to automatically provision and de-provision employee accounts.
Non-Technical:	● Customer must notify the Department of Information Technology Office of Security Management (DoIT OSM) of the Agency's interest in obtaining Security Awareness Training for agency employees and contingent workers ● Customer must identify the Agency Security Awareness Training Manager

	● Customer must provide the DoIT/OSM Security Awareness Training Administrators with the required Agency Memo acknowledging the Agency participation in security awareness training and identifying the primary and backup Agency Security Awareness Training Managers ● Customer must provide the DoIT/OSM Security Awareness Training Administrators with an excel.csv file of all Agency employees and contingent workers to be assigned security awareness training. ● Customer must provide the DoIT/OSM Security Awareness Training Administrators with up-to-date agency employee 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 OSM shall be responsible for the following activities in coordination with the customer receiving DoIT Security Awareness Training services:

1. Provide full administration of the security awareness training platform
2. Configure the security awareness training campaign and assessment for the customer
3. Configure training reminders for customer employees enrolled in security awareness training campaigns.
4. Upload the customer employee and contingent worker information (Excel.csv file) to the security awareness training platform when received from the Agency Security Awareness Training Manager.
5. Provide the customer with security awareness training progress reports
6. Provide vendor contract management
7. Maintain security awareness training learner licenses and monitor consumption
8. Serve as the escalation point for security awareness training platform and campaign issues
9. Provide security awareness training support: M-F, 8 am - 5 pm

10. Create customer employee progress reports (Reports will be scheduled to run on a schedule agreed upon with the Agency Security Awareness Managers)

11. Create the Quarterly Security Awareness Training Reports for the Governor's Office as stated in SB553.

12. Retain the required Agency Memorandum of Understanding (Memo) acknowledging enrollment in Quarterly Security Awareness Training and identifying the Agency Security Awareness Training Manager as stated in SB553. (Required Documentation)

B. Customer Responsibilities

The customer shall be responsible for the following activities:

1. Identify an Agency Security Awareness Training Manager.

2. Maintain updated employee information (including employee additions, deletions, and changes in employment status) for Department/Agency users being provisioned and de-provisioned in the security awareness training platform.

3. Submit support tickets to the DoIT Service Desk with updated employee information for all learners in an Excel.csv file. (The file shall contain all active employees and contingent worker information including First Name, Last Name, Email Address, and Agency/Department).

   a) Note: Okta Active Sync connected agencies are not required to submit CSV files for new employees and contingent worker account additions. Agency Security Awareness Training Managers are required to submit Excel.csv files for all employees and contingent worker account deletions and changes.

4. (Optional) Configure the Department/Agency identity provider to integrate with the security awareness training platform to permit automated account synchronization.

5. Ensure the Department/Agency maintains a 100% completion rate for all DoIT OSM-assigned training campaigns.

6. Send ad hoc notifications to Department/Agency employees to reinforce training and completion requirements.

IV. Service Level Agreements (SLAs)

A. Availability

The Department of Information Technology Security Awareness Training platform is a Software as a Service (SaaS) product. The Security Awareness Training platform availability is solely 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 OSM service targets with the SaaS vendor.

Category	Measure
Availability	Security awareness training platform availability target is 99.9% for 24x7x365 ● DoIT OSM Security Awareness Training Administrator support: M-F, 8 am - 5 pm, excluding state-approved holidays ● MDSOC incident support: 24x7x365

B. Maintenance

Scheduled Maintenance

The Security Awareness Training platform SaaS vendor is solely 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/OSM Security Awareness Training 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 security awareness trainer within 1 business day of being assigned to the Security Training Service Now assignment group
Emergency Changes	Emergency changes will be assigned to a security awareness trainer immediately after being assigned to the Security Training 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. <u>Request Management</u>

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.

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, termination requires written authorization by the State Chief Information Security Officer (CISO). If approved, terminations will only be effective at the end of the fiscal year.

VIII. Warranty, Limitations, and Exclusions

A. N/A