SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

Subscribing Entity

For

Cyber Security - Security Awareness and Training Services (FY2021)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and subscribing entity ("Customer"). The parties agree as follows:

1 Services Covered

The Maryland Department of Information Technology (DoIT) offers Security Awareness Training through Infosec Institute INFOSEC IQ. Maryland law requires any personnel with access to security-sensitive information receive annual security overview training or refresher security training.

Training Content includes but is not limited to:

- Malware & Phishing
- Social Engineering
- Privacy & Personal Identifiable Information (PII)
- Mobile Security
- Password Security
- Compliance
- Physical Security & Hardware
- Secure Applications Development
- Web-Based Threats
- Privacy & Data Protection
- Personal Security
- Advanced Cybersecurity & Risk Management
- Network Security
- General Data Protection Regulation (GDPR)
- Health Insurance Portability & Accountability Act (HIPAA)
- Cloud Security
- Email Phishing Campaigns
- PhishSim, includes 1,000s of phishing templates in a variety of attack types and difficulty levels, including drive-by, attachment and data-entry attacks. New templates are added each week, helping you and your workforce stay ahead of the latest threats.

Specialized/additional Training modules are available through Infosec Institute at an additional cost.

Contact the DoIT Service Desk to have a ticket placed with the Security Team for further information and cost of specific services outside our current contract scope.

2 Parties Responsibilities

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the subscribing entity and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

2.1 Operations

2.1.1 DoIT will:

- Provide contract management services with the vendor
- Configure reporting for agency training managers
- Provide training at least monthly to all agencies on a range of cybersecurity topics
- Include, at least annually, assessments designed to evaluate the effectiveness of the program.

2.1.2 The customer will:

- Submit a Security Awareness Training Plan identifying Agency assigned Security Awareness Managers to the DOIT Security Services, as required
- Assign a Security Awareness Training Manager for the agency. The Agency Security Awareness Manager is required to maintain updated employee information to include employee additions, deletions and changes in employment status.
- Submit a CSV File containing all active employee's and contractor's information including first name, last name, email address and Group/Agency before the Security Awareness Training can be configured. File should be submitted depending on frequency of changes. Smaller agencies once a month or as needed. Larger agencies with a lot of turnover may need to submit weekly updates.
- Communicate with Agency employees about the importance of this training as discussed in Senate Bill (SB)553.

3 Service Level Agreements

3.1 Availability

DoIT defines service availability for the managed firewall service as the system components being up and passing traffic with less than 10ms of delay.

3.1.1 Availability Target: 99%, measured monthly

The availability target excludes planned maintenance windows.

3.2 Incident Handling

3.2.1 Priority 1: Response time 2 hours, resolve time 24 hours

Priority 1 incidents include any issue that results in a total cessation of service.

3.2.2 Priority 2: Response time 4 hours, resolve time 2 days

Priority 2 incidents include any issue that results in a partial cessation or disruption of service, administrative access issues, and other important business issues.

3.2.3 Priority 3: Response time 2 business days, resolve time 5 business days

Priority 3 incidents include service questions, reporting, and other administrative issues such as user adds, deletes, and changes.

4 Maintenance Schedules

DoIT will provide notice to the User Agency at least 5 days in advance of any planned maintenance that impacts service availability.

5 Support and Service Outages

Service requests and security issues should be reported to the security operations center.

6 Costs for Services

The service pricing is based on consumption (named users). The cost per named user is $5.40, annually.

7 Termination of Services

The subscribing entity must provide 60 days advance written notice to terminate services. Termination of services will be effective at the end of the fiscal year following the conclusion of the 60-day notice period.

8 Warranty

No warranty is provided for this service.