SERVICE AGREEMENT

Between
The Maryland Department of Information Technology and
Subscribing Entity
For
Cybersecurity Shared 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

1.1 Shared-Value Services

The Department of Information Technology (DOIT) provides several services in the State's shared interests which are described in this service agreement.

1.1.1 Policy, Risk, and Governance

1. Development of Policy, Plans, Standards, and guidance
2. Development of data categorization standards
3. Consulting related to state security policy, audit compliance, and procurement requirements.
4. Development and refinement of incident response standards and processes
5. Review and oversight of unit-level security standards, plans, and procedures.
6. Handling and adjudication of security requests and incident reports.
7. Identify risks cogent to the State's mission and work with units to resolve.

1.1.2 Reporting and Oversight for Security Awareness and Training

1. Management and Oversight of Security Awareness and Training
2. Participation in local, regional, statewide and national cybersecurity exercises and events

1.1.3 Threat and Vulnerability Sharing

1. Dissemination of targeted threat intelligence received from third parties
2. Identification of vulnerable systems through third party and internal scanning tools
3. Aggregation and dissemination of threats emanating from State networks and resources
4. Management of the State's RiskSense statewide security risk scoring and management platform
5. Security scanning of shared infrastructure and services (e.g., Statewide DNS)
6. Ongoing operational projects to improve the security of the State's shared systems
7. Staffing for a Security Operations Center (SOC), where 24 x 7 x 365 monitoring and staffing ensures the highest level of network protection against.
8. Excludes the vulnerability management service

1.1.4 Incident Handling and Management

1. Provide response and recovery support for mass incidents, including DDoS and other large-impact events
2. Coordination of resources for cyber-disruptions

1.2 Standalone Services

For FY2021, the following services are add-ons that may be included in the single line item, for those units that subscribe.

1. Managed Firewall Service with SOC
2. Managed Vulnerability Service
3. Security Awareness and Training
4. Managed SIEM

2 Parties Responsibilities

For shared services, the unit's responsibilities are described in State law and in DoIT policy.

For standalone services, the product service agreements describe each party's responsibilities.

3 Service Level Agreements

For shared-value services, there are no service level agreements.

For standalone services, each product's service agreement describes the applicable SLAs.

4 Maintenance Schedules

For shared-value services, there are no maintenance schedules.

For standalone services, each product's service agreement describes the maintenance schedules.

5 Support and Service Outages

For standalone services, each product's service agreement describes the SLAs.

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

6 Costs for Services

For standalone services, each product's service agreement describes the costs and terms.

The cost for shared-value services is $95.00 per pin in the unit's legislative appropriation, and includes the costs for all shared-value services:

7 Termination of Services

For standalone services, each product's service agreement describes the conditions for terminating service.

Due to the nature of the shared-value services, there is no option to opt-out or terminate services.

8 Warranty

For standalone services, each product's service agreement describes the warranty.