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

Managed Firewall Services

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 Infrastructure Managed Firewall service is a comprehensive security solution. It includes a DoIT-managed perimeter Palo Alto Networks firewall that helps customers control network traffic based on their requested firewall rules. Additionally, it protects customer resources from malicious attacks using an intrusion prevention system (IPS), advanced threat protection, advanced URL filtering, malware protection, application control, and virtual private network (VPN) access.

The firewall pair provided in this service is located at two separate world-class data centers in Maryland and are monitored 24x7x365 for security events by the Maryland Security Operations Center (MDSOC). The DoIT firewall team is responsible for implementing all customer-requested firewall rule changes, monitoring security events, maintaining the health and availability of the firewall infrastructure, performing software and hardware upgrades, managing firewall licenses, and assisting the customers with troubleshooting network traffic issues.

A. Standard Service:

The following components are included with the standard service:

1. Highly available Palo Alto Networks firewall pair
2. DoIT Infrastructure Managed Firewall support team
3. MDSOC 24x7x365 security incident monitoring
4. Palo Alto Networks support
5. A custom built virtual firewall based upon customer preferences
6. Virtual Private Network (VPN) configuration

7. Intrusion Prevention System (IPS)
8. Advanced URL filtering
9. Malware protection
10. Application control
11. Onboarding and read-only account provisioning
12. Customer access to the firewall to review rules and logs
13. Policy management for routine and emergency changes
14. Change management
15. Problem management
16. Log retention for one (1) year
17. Firewall infrastructure maintenance (hardware and software)
18. Configuration backups
19. Annual Configuration Compliance Review
20. Customer audit support
21. Virtual Private Network (VPN) connectivity for DoIT managed workstations to the state network.

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Administrative access beyond view-only access to customer policies.
2. Customer application support, such as configuring websites, applications, databases, and Commercial Off-The-Shelf (COTS) software.
3. Validation of customer provided rule sets beyond identifying basic syntax errors and rules that violate State policies and industry best practices.
4. Custom report generation.
5. Troubleshooting local customer endpoint connectivity issues unrelated to the service (e.g., remote WIFI connection, off-premise networks).
6. User behavior monitoring not related to a security event.
7. VPN connections for non-hosted workstations

C. Optional Services

N/A

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 ● networkMaryland connectivity ● Okta Panorama Authentication ● DoIT Service Desk ● Maryland Security Operations Center (MDSOC) ● Managed workstations

Technical:	● **Network:** Local area network and routing is configured ● **Access:** Designated customer personnel can access Panorama using view-only accounts ● **Availability:** It is assumed that the Palo Alto Networks firewall will be operational and available to transport network traffic and protect customer resources ● **Connectivity:** It is assumed that the Palo Alto Networks firewalls have connectivity in the data centers. ● **Scalability:** It is assumed that the Palo Alto Networks firewalls can scale to accommodate the customer's evolving security needs
Non-Technical:	● Provide 24x7x365 points of contact (3) for coordinating outages, emergency maintenance/restoration, and change management ● Acceptance of Managed Services agreement and standard SOW ● Submit firewall rule changes using the DoIT defined change management process

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 (Network Managed Agencies)

DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

1. Develop the statement of work (SOW) for the Managed Firewall service.
2. Monitor firewall security events 24x7x365 and escalate issues in accordance with the DoIT incident response plan.
3. Create custom firewall policies built to meet the customer's specifications.
4. Provision Panorama access for approved users.
5. Bear the cost of maintaining the Palo Alto Networks subscription and support licenses.
6. Implement customer requested changes [routine and emergency] following DoIT's change management procedures.
7. Maintain backups of the customer's firewall configuration every 24 hours.
8. Schedule maintenance and notify customers when the firewall infrastructure (firewall, log collector, Panorama) will be unavailable due to maintenance.
9. Initiate and fulfill the return materials authorization ("RMA") process with Palo Alto Networks in the event that the hardware/software is determined to be in a failed or faulty state and requires replacement.

10. Patch and upgrade the firewall infrastructure operating system versions.
11. Troubleshoot and replace firewall hardware components that fail or are no longer supported.
12. Complete the Annual Configuration Compliance Review (ACCR), yearly.
13. Provide audit support to customers by sharing the customer's firewall configuration with authorized auditors.
14. Install and maintain the Global Protect VPN client on endpoints.

B. <u>DoIT Responsibilities for Customer (Self Managed Network/Workstation Agencies)</u>

DoIT shall be responsible for the following activities in coordination with the Customer for which DoIT does not provide enterprise managed services:

1. Develop the statement of work (SOW) for the Managed Firewall service.
2. Monitor firewall security events 24x7x365 and escalate issues in accordance with the DoIT incident response plan.
3. Create custom firewall policies built to meet the customer's specifications.
4. Provision Panorama access for approved users.
5. Bear the cost of maintaining the Palo Alto Networks support licenses.
6. Implement customer requested changes [routine and emergency] following DoIT's change management procedures.
7. Maintain near real-time backups of the customer's firewall configuration.
8. Schedule maintenance and notify customers when the firewall infrastructure (firewall, log collector, Panorama) will be unavailable due to maintenance.
9. Initiate and fulfill the return materials authorization ("RMA") process with Palo Alto Networks in the event that the hardware/software is determined to be in a failed or faulty state and requires replacement.
10. Patch and upgrade the firewall infrastructure operating system versions.
11. Troubleshoot and replace firewall hardware components that fail or are no longer supported.
12. Complete the Annual Configuration Compliance Review (ACCR), yearly.
13. Provide audit support to customers by sharing the customer's firewall configuration with authorized auditors.

C. <u>Customer Responsibilities</u>

The Customer shall be responsible for the following activities:

1. Sign the statement of work (SOW) for the Managed Firewall service.
2. Provide all required information to implement a firewall rule change.
3. Respond to firewall incident escalations, in a timely manner, to validate suspicious activity, provide context, and support response and remediation efforts.
4. Provide 24x7x365 three (3) points of contact (escalation contacts) for coordinating outages, emergency maintenance/restoration, and change

management.

5. Designate the point of contacts authorized to approve firewall rule changes and provide the list to DoIT.
6. Ensure the availability of customer firewall approvers during business hours.
7. Promptly notify DoIT of any changes to the designated escalation contacts and customer firewall approvers. Changes may include, but are not limited to, updates in contact information, changes in the designated individuals responsible for escalation, or the addition/removal of escalation contacts.
8. Ensure testers perform all necessary tests within three (3) days after an approved firewall change has been implemented.
9. The customer is responsible for submitting a new ticket after an existing ticket has been automatically closed due to no response from the customer, after three (3) days.
10. The customer firewall approver must approve authorized user access to Panorama.
11. Request the rescheduling of routine maintenance within four (4) calendar days of the maintenance date. (Emergency maintenance cannot be stopped by the customer.)
12. Provide resources to support and complete the Annual Configuration Compliance Review (ACCR), in a timely manner.
13. Submit a ticket requesting firewall audit support two (2) weeks in advance of the date support is needed, at a minimum.
14. (Non-managed Agencies) Install and maintain the Global Protect VPN client on endpoints.
15. The customer is responsible for coordinating communication with any third-party partners.

IV. Service Level Agreements (SLA’s)

A. Availability

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 DoIT’s service targets.

Category	**Measure**
Availability	Firewall availability target is 99.9% for 24x7x365 ● DoIT Infrastructure MFW support: M-F, 8AM - 5PM, excluding state approved holidays ● MDSOC incident support: 24x7x365

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 (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.

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**
Normal Changes	Normal changes will be assigned to a firewall administrator within 1 business day of being assigned to the Managed Firewall Admins assignment group
Emergency Changes	Emergency changes will be assigned to a firewall administrator immediately after being assigned to the Managed Firewall Admins assignment group

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	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 work around 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 work around is available ● An issue is affecting a single user that is not business critical or time sensitive	4 business days	7 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 the quantity of licenses or relocation of service.
      - 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.

3. Firewall Rule Modifications
   To add, modify, or delete a firewall rule, the Customer must:
   a) Submit a request via email with the attached Firewall Change Request Form to soc.doit@maryland.gov with the subject line "<your agency> - Firewall Change Request" to ensure it is classified properly.

- For urgent requests, please call the MDSOC (410-697-9700) after you receive a ticket number and request escalation.

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. For FY26, 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. Future years will transition to a reimbursable cost model as described below.

A. Costs are identified through a sizing model (small, medium, and large).Costs will vary by the size of the agency in terms of State PINS/contractor support. Current structure is as follows:

The cost of firewalls is allocated based on the size of the agency, which is determined by the number of PINs associated with the agency. The total firewall cost includes labor, licensing, hardware, and Palo Alto support.

This allocation model ensures that firewall expenses are distributed proportionally based on agency size, as calculated from the agency's PIN count.

1. Small (< 50 PINS/contractor support)
2. Medium (50-500 PINS/contractor support)
3. Large (> 500 PINS/contractor support)

B. VPN services are inclusive of the managed firewall service for managed agencies

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 to 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