Mississippi Department of Information Technology Services	**Doc Ref Number:** ESW-PSG-3004	
	Title: Virtual Private Network (VPN) Standard	
	Document Type: Enterprise Statewide	**Page:** 1 of 2
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 6/13/2025	**Revision Date:** 6/13/2025

1. AUTHORITY

The Mississippi Department of Information Technology Services (ITS) shall provide coordinated oversight of the cybersecurity efforts across all state agencies, including cybersecurity systems, services and development of policies, standards, and guidelines (§ 25-53-201).

2. PURPOSE

This document formally promulgates the ITS-managed enterprise virtual private network (VPN) as the enterprise standard for all virtual circuits connecting the Enterprise State Network to external locations. "Virtual circuits" includes both client and network-based circuits, and "external locations" means any location that does not connect exclusively to the Enterprise State Network whether the location is third party or state.

3. SCOPE

This standard applies to all state agencies and their employees; trusted partners; or any entity (as provided by law) authorized to operate, manage, or use State of Mississippi information and information technology (IT) systems (hereafter referred to collectively as “SOM Assets”). Agency is defined as and includes all the various state agencies, officers, departments, boards, commissions, offices, and institutions of the state (§ 25-53-3 (2)(e)).

4. OVERVIEW

To advance the enterprise approach to cybersecurity, ITS established the enterprise VPN solution as the standard for state agencies. Consolidating VPN management for state government has reduced the potential attack surface by minimizing the number of inbound open ports in the state’s security border. This enhances security by providing consistent encryption and access controls across the enterprise state network. It simplifies network management by centralizing configuration, monitoring, and updates, ensuring compliance with security policies.

4.1. The solution is purchased by ITS therefore reducing the costs to state agencies for specific utilizing of the core functionality. Key features of the solution include:

- 4.1.1. Support (24x7) both client-based VPN tunnels and site-to-site VPN tunnels
- 4.1.2. Enforce multi-factor authentication for all client-based VPNs
- 4.1.3. Enforce disablement of split tunneling, prohibiting client-based VPNs from having the ability to participate in a LAN while also connected to the Enterprise State Network via VPN
- 4.1.4. Internet access is only allowed for approved business sites
- 4.1.5. Utilize ITS-approved encryption protocols
- 4.1.6. Ability to evaluate the security health of client VPN devices before granting network connectivity

4.1.7. Redundancy and business continuity plans to maintain capability in the event of a disaster affecting both State Data Centers

5. Billing

Agencies shall be billed for their utilization of the enterprise VPN solution.

5.1. Each agency is responsible for identifying the need for client and site-to-site VPN tunnels and associated service options required by their agency

5.2. The type of services that are billed to agencies include:

5.2.1. Monthly Client VPN Accounts
5.2.2. Monthly Site-to-Site Tunnels
5.2.3. Physical Multi-factor Tokens
5.2.4. Trouble Requests
5.2.5. Change Requests
5.2.6. Compliance Configuration Charges

5.3. For more details regarding applicable charges, agencies must submit a request to the ITS Service Center.

6. STANDARD

6.1. Each agency must participate in the enterprise VPN solution for virtual circuits connected to the Enterprise State Network.

6.1.1. The only exceptions permitted to this standard are those that are approved in writing by ITS for an agency's specific purpose and are only applicable to that agency's operations for the duration of time defined by the exception.