Mississippi Department of Information Technology Services	**Doc Ref Number:** ESW-PSG-3005	
	Title: Agency Firewall Standard	
	Document Type: Enterprise Statewide	**Page:** 1 of 1
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 10/03/2025	**Revision Date:** 10/03/2025

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 establishes the official firewall standard for state agencies that connect to the enterprise state network.

3. SCOPE

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

4. OVERVIEW

To support a unified enterprise approach to cybersecurity, ITS is responsible for designing and managing the enterprise state network under a shared responsibility model. This responsibility includes maintaining an enterprise security border that separates and protects the enterprise state network from the public Internet.

The enterprise security border consists of technologies such as firewalls, intrusion prevention systems, reverse proxies, and additional security sensors and components. Managed by ITS, this security framework provides a protected environment while enabling secure communication among state agencies participating in the semi-trusted shared network, known as StateNet.

5. STANDARD

5.1. Each agency must implement one or more firewalls at the logical demarcation points between StateNet and their agency assets.

5.1.1. Common points of demarcation are but not limited to:

5.1.1.1. At the border of the agencies local network (including remote sites)

5.1.1.2. Within the ITS public cloud landing zones to protect individual workloads