Mississippi Department of Information Technology Services	**Doc Ref Number:** ESW-PSG-3006	
	Title: Enterprise Guest-Public Access to State Network	
	Document Type: Enterprise Statewide	**Page:** 1 of 2
	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 requirements for ensuring that guest/public users are prohibited from accessing state network resources. To facilitate guest/public access, ITS has approved several methods for providing Internet access to guest users while maintaining compliance with state cybersecurity policies.

3. SCOPE

This standard applies to all state agencies on the Enterprise State Network 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, state agencies must implement security controls to prevent guest/public users from accessing state government resources on the Enterprise State Network. Allowing guest or public users to access a government network and IT resources creates significant cybersecurity risks, including potential unauthorized access to sensitive data, introduction of malware or ransomware, and exploitation of network vulnerabilities. Such access also makes it harder to monitor, control, and contain threats, increasing the likelihood of data breaches and service disruptions.

5. STANDARD

5.1. Each agency must prohibit guests and public users from accessing internal State Network resources.

5.2. Each agency on the Enterprise State Network that is required to provide Internet access for guests and public users must implement one of the following ITS-approved connectivity methods:

5.2.1. **Method 1:** Install a dedicated circuit and separate networking equipment for guest users. Agencies must coordinate with ITS to implement this solution.

5.2.2. **Method 2:** Use an ITS approved technology to tunnel all guest user traffic to an ITS-managed Demilitarized Zone (DMZ). Those options include:

5.2.2.1. Utilizing the ITS-managed Cisco solution
5.2.2.2. Utilizing the ITS-managed Aruba solution
5.2.2.3. Installing a Cisco Meraki in the ITS Data Center and providing ITS network staff read-only access to verify configuration

5.2.3. Each agency must implement the following security controls if they choose to utilize either of the approved methods listed in item 5.2.

5.2.3.1. **Inbound Access**: No inbound ports may be opened to guest users.
5.2.3.2. **Traffic Filtering:** All traffic originating from guest users must be filtered through approved security measures. Guest networks are also required to block any prohibited technology- https://www.its.ms.gov/services/security/prohibited-technology

5.2.4. Each agency that decides to allow guests and public users access to State Network resources must contact ITS for assistance to ensure that the solution is compliant with this standard.