

	<b>Doc Ref Number:</b> ESW-PSG-3003	
	<b>Title:</b> Email Gateway Solution Standard	
	<b>Document Type:</b> Enterprise Statewide	<b>Page:</b> 1 of 2
	<b>Domain:</b> Security   Compliance	<b>Status:</b> Approved
	<b>Effective Date:</b> 6/13/2025	<b>Revision Date:</b> 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 email gateway as the enterprise standard for consolidating email security management for state government.

**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 email gateway solution as the standard for state agencies. By consolidating email security management for state government, ITS can consistently monitor for potential threats and swiftly respond to security incidents, ensuring heightened visibility and a uniform defense against evolving cyber threats.

The enterprise email gateway solution provides comprehensive inbound and outbound email filtering, alongside enhanced security features such as anti-spam, URL defense, DKIM, SPF, and regular DMARC checks.

The solution is purchased by ITS and there are no costs to state agencies for utilizing the core functionality. ITS continue to explore add-on features that state agencies may find beneficial for specific needs. Additional features beyond the core functionality may incur costs that elect to utilize them. Core functionality of the solution include.

4.1 Centralized Visibility and Management - Streamlined administration with a centralized platform for managing email accounts, security policies, and user access. This ensures consistent and efficient email management across the organization.

4.2 Advanced Authentication Protocols - Implementation of industry-standard authentication protocols, including DKIM and SPF, to enhance email security and prevent unauthorized access, ensuring the authenticity of outgoing emails. Many organizations across various sectors are adopting these authentication protocols to combat email-based attacks effectively.

4.3 DMARC Integration – The enterprise solution incorporates DMARC (Domain-based Message Authentication, Reporting, and Conformance) to provide an additional layer

<b>Doc Ref Number:</b>	ESW-PSG-3003	Pending
<b>Document Type:</b>	Enterprise Statewide	<b>Page:</b> 2 of 2
<b>Title:</b>	Email Gateway Solution Standard	

of protection against phishing attacks and email spoofing. This contributes to the overall trustworthiness of our email communications. DMARC adoption plays a crucial role in improving the overall security posture of organizations and the broader email ecosystem. Leading organizations are leveraging DMARC to enhance email security and reduce the risk of phishing attacks. Our commitment to regular DMARC checks positions us as proactive contributors to the overall improvement of email security practices. By aligning with these trends and best practices, we ensure that our email communications maintain a high level of authenticity and trustworthiness.

4.4 Scalability and Flexibility - The framework of the enterprise email solution serves as a foundation, providing a secure and reliable baseline for email communication. Recognizing that different agencies may have unique security requirements, the solution is intentionally designed to allow the addition of supplementary security features like end-to-end encryption at an added cost.

## **5. STANDARD**

5.1. Each agency must use the enterprise email gateway solution for all inbound and outbound email.

5.1.1. 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.