ITS Operations Privileged Access Policy

Notice of Approval

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3008	
	Title: ITS Operations Privileged Access Policy	
	Document Type: ITS Operational	
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: March 1, 2018	**Revision Date:** March 1, 2018

Notice is hereby given, that the above specified document meets the requirements of the Mississippi Department of Information Technology Services Policies, Standards and Guidelines Program, defined in ESW-PSG-1001, thereby warranting approval for implementation, effective immediately.

Executive Director
Mississippi Department of
Information Technology Services

March 1, 2018
Date of Signature

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3008	
	Title: ITS Operations Privileged Access Policy	
	Document Type: ITS Agency	**Page:** 1 of 2
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 03/01/2018	**Revision Date:**

1. AUTHORITY

The Mississippi Department of Information Technology Services (ITS) shall issue recommended strategies and goals for the effective and efficient use of information technology and services in state government (§ 25-53-29(2)). Additionally, ITS shall publish written planning guides, policies and procedures for use by agencies and institutions in planning future electronic information service systems (§ 25-53-29(1) (b)).

2. PURPOSE

The purpose of this document is to establish and document the standards and guidelines for reviewing and confirming privileged access to firewalls maintained by ITS Operations. Access control is considered the first barrier in protecting critical IT resources and data.

3. SCOPE

Privileged access, commonly referred to as supervisor, administrator, admin, or root access, allows an individual full permissions to the resources within their authority. This policy is limited to ITS Operations privileged access.

4. POLICY

The State of Mississippi, Information Technology Services, shall have effective standards and guidelines for physical and logical procedures for protection of hardware, software, networking, and support equipment that stores and processes data for state agencies where ITS Operations has visibility and access to the data. This policy informs ITS Operation's administrators at all levels of the inherent obligations and responsibilities that accompany privileged access.

4.1 The ITS Operations Officer and ITS Operations Directors shall maintain a list of each privileged user account and related systems

4.2 Multi-factor authentication should be considered for all privileged user accounts. Justification for not implementing multi-factor authentication should be completed and provided to the ITS Operations Officer for each system not implementing multi-factor authentication

5. STANDARDS

5.1 Privileged access shall only be granted to authorized individuals using principles of minimal privilege needed

5.2 Administrators shall not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.

5.3 There shall be a bi-annual (every six months) privileged user account audit performed by the responsible ITS Director to verify account credibility and to change the passwords on the existing privileged user accounts. The ITS Director will furnish the report to the ITS Operations Officer

6. GUIDELINES

6.1 Privileged access should be requested and authorized by the responsible ITS Director. Substantial justification is required for approval. An authorized administrator is responsible for creating the privileged account. All normal user ID and password policies and procedures apply.

6.2 Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties.

6.3 User with privileged access should report unusual or unauthorized activity to the ITS Security Team.

6.4 Users with privileged access should always be aware that these privileges place them in a position of considerable trust. Users must not breach that trust by misusing privileges or failing to maintain a high professional standard.

7. REFERENCES

§ 25-53-29 (2)
§ 25-53-29 (1) (b)