# ITS Operations Firewall Rule Policy

# Notice of Approval

| | | |
|---|---|---|
| Mississippi Department of Information Technology Services | **Doc Ref Number:** ITS-PS-3007 | |
| | **Title:** ITS Operations Firewall Rule 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-PS-3007 | |
| | **Title:** ITS Operations Firewall Rule Policy | |
| | **Document Type:** ITS Agency | **Page:** 1 of 2 |
| | **Domain:** Security \| Compliance | **Status:** Approved |
| | **Effective Date:** March 1, 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 firewall rules sets maintained by ITS Operations. Firewall rules sets are a critical barrier in protecting State of Mississippi resources and data. Firewalls are an essential component of the information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services and establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information.

## 3. SCOPE

This policy is limited to firewall and firewall rules sets maintained by ITS Operations.

## 4. POLICY

The State of Mississippi, Information Technology Services, shall have effective procedures for physical and logical procedures for protection of hardware, software, networking, and support equipment that stores and processes data for authorized agencies of the State of Mississippi. This policy informs administrators at all levels of the inherent obligations and responsibilities of creating, maintaining, and administering firewall rules.

**4.1** All firewall changes including rule additions or deletion shall be approved by an ITS employee in a management position or designated by a manager.

**4.2** Only authorized firewall administrators shall make all approved changes.

**4.3** Logs - All changes to firewall configuration parameters, enabled services, and permitted connectivity paths should be logged

## 5. STANDARDS

**5.1** There shall be a bi-annual (every six months) review of firewall changes performed by the responsible ITS Director to verify credibility and

documentation of changes.

**5.2** All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also should be logged. These logs should be maintained in a recording system and stored at least 12 months or longer, where required, after the time they were recorded. These logs should be reviewed on a regularly schedule to ensure that the firewalls are operating in a secure manner.

**5.3** Contingency Planning – ITS staff responsible for firewalls should prepare and obtain ITS approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability.

**5.4** Firewall Change Control - Because firewalls support critical information system activities, firewalls are considered a production system. All changes to the firewall software provided by vendors, excluding vendor-provided upgrades and patches and fixes should be considered a standard change in the Change Management Process.

**5.5** If possible, the responsible ITS Director should utilize a technical expert to assist with the bi-annual mainframe firewall change review.

## 6. REFERENCES

§ 25-53-29 (2)
§ 25-53-29 (1) (b)