MISSISSIPPI STATE UNIVERSITY

OP 30.04: NETWORK INFRASTRUCTURE AND FIREWALLS

PURPOSE

The purpose of this Operating Policy is to define the essential rules regarding the secure management and maintenance of the campus network at Mississippi State University (MSU).

The network securely integrates voice, data, video, e-commerce and wireless applications into a powerful, unified information technology resource upon which our students, faculty and staff depend.

The elements of our network infrastructure include:

- The outside network cable plant (e.g., fiber-optic cable, copper twisted-pair cable, and associated electronics)
- Building network cabling systems (e.g., wiring closets, data and telephone cable and faceplates)
- Network electronic components (e.g., switches, routers, hubs, repeaters and transmission equipment)
- Network protocols, services, addressing and naming conventions (e.g. IP, DHCP, DNS, SNMP, H.323, SIP)
- Security and authentication services (e.g., LDAP, PKI, CAS, Active Directory)
- Firewalls
- Wireless networking (e.g., indoor and outdoor access points)
- ID Card systems (e.g., card readers, access control applications, and card production systems)
- External network connections (e.g., Internet, Internet2, the Public Switched Telephone Network, and VoIP)

The size, complexity, and mission-critical role of the network demand adherence to a centralized, coordinated strategy for planning, implementation, operation, and support. Such a strategy is necessary to protect the future reliability, maintainability, and security of this critical asset.

POLICY

The university will have an institution-wide strategy for maintaining and enhancing the network infrastructure with Information Technology Services (ITS) having overall responsibility for planning, setting of standards, implementation, operation, and support of the infrastructure. Implicit in this responsibility is the authority of ITS to take necessary preventative and remedial steps to ensure the operational integrity of the network and underlying infrastructure.

It is the policy of Mississippi State University to protect critical information in all forms for which it is the custodian. To achieve this policy, it is essential to provide secure, managed, and tested firewall configurations to protect university Information Technology (IT) resources.

It is the goal of the university to have in every university building an appropriately networked secure data infrastructure that is consistent with the standards and practices of the institution. New building construction and major building renovations will include funding for a fully networked data infrastructure. For existing buildings, infrastructure plans will be developed and all network enhancements, regardless of source of funds, will be consistent with those plans.

While Information Technology Services (ITS) has overall responsibility for planning, setting of standards, implementation, operation, and support of the network infrastructure, including firewalls at MSU, management may be distributed into units who have the staffing and expertise to administer this mission-critical infrastructure service.

Adherence to this policy is required of all units who support network equipment and firewall hardware/configuration at Mississippi State University.

Exceptions to this policy may be granted by the President.

PROCEDURE

For ***new buildings and buildings undergoing major renovation***, the following procedure should be followed:

- During budget planning, representatives of Information Technology Services will meet with the building occupants and the architect to develop a budget allocation consistent with the networking needs of the building. This budget estimate will be changed in the final budget only with an approved modification of the planned network infrastructure.
- As the detailed design of the building is developed by the architect, Information Technology Services will continue to work with the architect and the building occupants to develop the detailed specification of the building network. This includes wiring, electronics, location and size of wiring closets, location and nature of connections for use within the building, and connectivity to the university's backbone.
- ITS staff will participate in overseeing the installation of the network and in inspections involving components of the network infrastructure.
- Once accepted, ITS will assume operational responsibility of the network infrastructure (but not, without special arrangements, the end-user facilities).
- ITS will coordinate the overall network project with other university units, e.g., Facilities Management. One-time and recurring costs and funding sources will be identified, as appropriate, during the planning phase.
- Individuals or departments wishing to enhance the network infrastructure in an existing building must first contact ITS.

All units must provide the following essential elements of information security best practice in firewall management and maintenance on the MSU network:

- Monitoring Vulnerabilities – Firewall devices must be patched in a timely fashion and vulnerabilities relevant to the MSU environment must be promptly addressed.

- Rules
    - All networks must at a minimum provide inbound “deny all” rules such that inbound traffic requires explicit approval.
    - All high-risk networks as defined by standards or internal policy must contain “deny all” outbound rules such that outbound traffic requires explicit approval.
    - Rules that open services to the Internet at large must be reviewed with particular care on an annual basis.
- Change Management – Any request for rule changes must be reviewed from a security risk perspective and follow an explicit, documented approval process that is appropriate for the unit managing the firewall. The following minimum elements shall be enforced:
    - All requests are logged with rule information, and a listing of the approver, requestor, and implementor.
    - No user may both request and approve a firewall change except in an emergency.
    - Emergency changes must be logged and approved retroactively.
    - All rules must be tested periodically.
- Firewall Logs – Logs must contain both host block information and relevant administrative information such as changes or administrative actions.
    - Units must document and implement a process of periodic log review to ensure secure operation of the firewall.
    - Logs must be maintained for a minimum of 6 months.
- Audit Requirements – Rules must be reviewed annually to ensure that existing rules are still required and relevant.

REVIEW

This policy will be reviewed at least every four years by the Chief Information Officer with recommendations for revision presented to the Provost and Executive Vice President.

REVIEWED BY:

/s/ Steve Parrott 11/22/2021
Chief Information Officer Date

/s/ David Shaw 11/22/2021
Provost and Executive Vice President Date

/s/ Tracey Baham 11/22/2021
Assistant Vice President, Institutional Strategy & Effectiveness Date

/s/ Joan Lucas 11/22/2021
General Counsel Date

APPROVED:

/s/ Mark Keenum 11/22/2021
President Date