**Purpose**

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Rule set. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either “Network” or “Host”: a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

**Scope**

This policy applies to all firewalls on Morehouse School of Medicine (MSM) networks, whether managed by employees or by third parties. Departures from this policy will be permitted only if approved in advance and in writing by the IT Infrastructure Service Director.

1. Provide guidance on when firewalls are required or recommended. A Network Firewall is required in all instances where Sensitive Data is stored or processed. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.
2. Raise awareness on the importance of a properly configured (installed and maintained) firewall.

**Definition**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Electronic Equipment: | All MSM-owned or issued and any personally-owned computer or related equipment (e.g., servers, workstations, laptops, PDAs, printers, fax and other such devices) that attaches to the MSM network, or is used to capture, process or store MSM data, or is used in the conduct of MSM business. |
| Enterprise System: | Applicable to any infrastructure as a means of describing its importance to the MSM's mission and how it should be administered, protected and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to a very broad constituency spanning organizational boundaries. An Enterprise System is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered. |
| Firewall: | Any hardware and/or software designed to examine network traffic using policy statements (rule set) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment. |
| Firewall Administrator: | The MSM personal charged with the responsibility of Firewall Configuration and/or Rule set administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rule sets. |
| Firewall Configuration: | The system settings affecting the operation of a firewall appliance. |
| Firewall Rule set: | A set of policy statements or instructions used by a firewall to filter network traffic. |
| Host: | Any computer connected to a network. |
| Host Firewall: | A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec’s Norton Personal Firewall, Zone Labs’ ZoneAlarm, native firewall functionality supplied under operating systems, e.g., Mac OS X, Linux, Windows 7 (and higher). |
| Internal Information: | Information that is intended for use by and made available to members of the MSM community who have a business need to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need. MSM reserves the right to control the content and format of Internal information when it is published to external parties. Examples include employment data, financial expenditure detail, Course Teacher Evaluations, patient records and Directory Information (not subject to a FERPA hold). |
| Legally/Contractually Restricted Information: | Information that is required to be protected by applicable law or statute (e.g., HIPAA, Georgia Personal Identity Protection Act), or which, if disclosed to the public could expose the MSM to legal or financial obligations. Examples include, but are not limited to, occurrences of personally-identifiable information, e.g., social security numbers (SSNs), personnel records, student records, medical records, names in connection with SSNs, and credit card numbers. Specific University policies may apply to particular data in this classification, e.g., Secure Handling of Social Security Numbers, Security of Electronic Protected Health Information, etc. |
| Network Device: | Any physical equipment attached to the MSM network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points. |
| Network Extension: | Any physical equipment attached to the MSM network designed to increase the port capacity (number of available ports) at the point of attachment. Examples include, but are not limited to: routers (wired and wireless), switches, hubs, gateways. |
| Network Firewall: | A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s). |
| Public Information: | Information that is available to all members of the MSM community, and may be released to the general public. The MSM reserves the right to control the content and format of Public Information. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Examples include the University's auditable financials, schedule of classes, and approved census facts. |
| Sensitive Data: | See “Legally/Contractually Restricted Information” above. |
| MSM Network: | The network infrastructure and associated devices provided or served by MSM. |
| **Policy Statement** |  |

Where Electronic Equipment is used to capture, process or store MSM data identified as “Legally/Contractually Restricted” and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is **required**.

All installations and implementations of and modifications to a Network Firewall, its Configurations or Rule set are the responsibility of the authorized MSM Firewall Administrator, with this exception: maintenance of a Network Firewall Rule set may be performed by persons/vendors other than MSM personnel where permitted by a documented agreement between MSM and the persons/vendors assuming the Firewall Administrator’s responsibilities.

**Procedures**

All Network Firewalls installed and implemented must conform to the current standards as determined by MSM. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

1. The Request for Firewall Rule set Modification Form is used to:
2. Request and document all changes to Network Firewall Rule sets where Firewall Administration is performed by Firewall Administrator. All requests are subject to the approval of Director of Infrastructure.
3. Document (only) all changes to Network Firewall Rule sets where Firewall Administration is performed by persons other than MSM. All requests are subject to review by Director of Infrastructure.
4. All related documentation is to be retained by the Firewall Administrator for three (3) years and is subject to review by MSM and Audit and Advisory Services.
5. All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial Rule set should be set to “logging or learning mode” to prevent service interruptions). The Rule set should be opened incrementally to only allow permissible traffic.
6. Firewalls must be installed within production environments where “Legally/Contractually Restricted Information” is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.
7. Firewall Rule sets and Configurations require periodic review to ensure they afford the required levels of protection:
8. Director of Infrastructure must review all Network Firewall Rule sets and Configurations during the initial implementation process.
9. Firewalls protecting Enterprise Systems must be reviewed semi-annually; MSM Firewall Administrators and Information Security must collaborate on this review.
10. Firewalls not protecting Enterprise Systems must be reviewed annually by the responsible Firewall Administrator.
11. Firewall Administrators must retain the results of Firewall reviews and supporting documentation for a period of three (3) years; all results and documentation are subject to review by MSM and Audit and Advisory Services.
12. Firewall Rule sets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rule sets and configurations and backup media must be restricted to those responsible for administration and review.
13. Any MSM entity operating under a clinical license is required to have properly configured Firewalls in place to protect electronic Personal Health Information (ePHI) and comply with HIPAA Standards. MSM Firewalls should include the use of Network Address Translation (NAT) where required to help ensure compliance with HIPAA. Any questions about the suitability and use of NAT should be directed to Information Security.
14. Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed at least daily, with logs retained for ninety (90) days. It is recommended that utilities or programs that facilitate the review process be employed. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.
15. MSM Firewall Administrators will execute approved changes to the Firewall Rule sets maintained by MSM during the scheduled maintenance window.
16. MSM Firewall Administrators will perform changes to Firewall Configurations according to approved production maintenance schedules.
17. Current offline back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times. A permissible alternative to offline copies involves online encrypted versions of these same files. Where systems software permits it, the automatic reestablishment of approved copies of these systems files must proceed whenever an unauthorized modification to these files has been detected.
18. MSM staff members responsible for managing firewalls should stay current with information about firewall vulnerabilities. Any vulnerability that appears to affect MSM networks and systems must promptly be brought to the attention of the IT Infrastructure Services Director.
19. MSM firewall must be located in locked rooms accessible only to those who perform authorized firewall management and maintenance tasks approved by the IT Infrastructure Services Director. The placement of firewalls in an open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable. The room that house the firewall device is equipped with an automated log of all persons who gain entry to the room.

**References**

NIST – 800-41 rev1, 800-53 rev 4

Recommended By:

Effective Date:

Authorized By:

Date of Last Edit:

Review Date: