POLICY NAME: Firewall Management Policy

Effective Date:	August 31, 2007
Policy Owner:	TSD
Policy Number:	TSD-NET1002
Related Policies:	State of Virginia ITRM Standard SEC501-01
Purpose:	The purpose of this policy is to ensure continuity of operations and maintenance of appropriate controls on firewalls and associated devices.
Scope:	Firewall Management Policy TSD-1002 applies to all firewalls and Virtual Private Network (VPN) gateways managed by TSD Network Engineering and Technology.
Policy Statement:	This policy defines the control and management of firewalls and VPN equipment administered by Network Engineering and Technology (NET), and used in the protection of Mason's network.
Definitions:	Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted. Virtual Private Network (VPN): a network available via the internet that allows individuals to share and access information privately and securely from any computer anywhere. VPN is used to allow persons to connect to Mason computer resources from home or other offsite location for the purpose of telework.
Responsibilities:	Responsibility for configuration management of resources at all

campuses of George Mason University resides with the Vice President for Information Technology. The Information Technology Unit's Network Engineering group, under the direction of the Vice President for Information Technology, is responsible for setting local standards and policies for the initial installation and changes to network firewalls.

Compliance:

All university employees, contractors, and business partners and all Network Engineering and Technology personnel responsible for initial installation and/or changes to network firewall configuration shall comply with this policy.

System owners must have documented Configuration Management procedures for firewall installation and change control and must be able to produce the documented procedures when required for auditing purposes. Evidence of Installation and Change Request procedure implementation must be available for auditing purposes.

Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action.

Implementation Process:

Preinstallation

- A system profile (generally using NET-A0020_A form) for each system to be installed in the Enterprise Core should be completed at least five working days prior to the requested activation date of the system or service. System profiles should detail network accessible services and protocols, authorized users, and any other characteristics required to adequately protect the resource(s). Completion of a system profile typically requires the host system administrator and/or application owner to work jointly with NET staff to identify the critical components and processes that are involved.
- TSD departments responsible for maintaining systems in the Enterprise Core may enter the system profile

information in the Change Management Database (CMDB) in lieu of using the NET-A0020_A form.

- Requests for VPN access must list authorized users by name, department, and GID number and be signed by a department manager, Dean, or Director.

Installation

- Firewalls and VPN equipment shall be configured in accordance with the applicable Network Device Security Guidelines.
- Management auditing and logging shall be implemented on all devices which support auditing and logging.
- Existing component-level network drawings and topology maps should be updated as soon as possible after a hardware change is made.

Configuration Changes

- Changes to the firewall device's hardware, software, or operating environment as well as any change to the rulebase shall be documented in accordance with TSD Policy NET-1001, Network Device Change Management.

Maintenance

- Administrative passwords for firewalls and associated devices shall, where possible, conform to current MESA requirements for structure and composition.
- A copy of administrative passwords for all firewalls shall be kept in the encrypted "Password Safe" application which is managed by Network Engineering and Technology.
- A backup of the currently installed firewall rule base must be made prior to implementing any rule changes.
- An explanation of each rule should be included with its rulebase entry.
- Audit logs shall be stored on clearly labeled media, and

must be retained for at least 12 months.

- An audit of system profiles on record and actual system configurations shall be completed annually.

Approved By:	Walt Sevon Deputy CIO Executive Director, Technology Systems division
Approval Date:	April 5, 2011
Revision History:	*N/A*
Supersedes (Previous Policy):	*N/A*
Date of Review:	April 1*, 2011*

Policy Contact Name:	David Robertson – Service Delivery Manager
Policy Contact E-mail:	