- **Policy Title** - Firewall Management

- **Policy ID -** TSD-1002

- **Version -** Version: 1.2

- **Supersedes –** Version 1.1

- **Review Date –** One (1) year from effective date.

- **Procedures -** Device Installation Guidelines, Network Configuration Management, Online forms NET**-**A0020_A "Firewall Change Request Form", NET-F0021_A Staff VPN Request, NET-F0020_A Vendor VPN Request

- **Overview --** This policy governs the control and management of firewalls and VPN equipment administered by Network Engineering and Technology (NET), and used in the protection of the University's network.

- **Purpose** - Ensure continuity of operations and maintenance of appropriate controls on firewalls and associated devices.

- **Applicability** - Applies to all firewalls and Virtual Private Network (VPN) gateways managed by TSD Network Engineering and Technology. The Enterprise Core firewall has additional requirements beyond those mandated for departmental or building/area firewalls, as noted below.

  - 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.

❖ Compliance

All NET personnel have a responsibility to comply with this policy. A requester's failure to provide an adequate level of information for the system profile or VPN authorization request may result in the delay or denial of the requested service.

Effective Date: 08/31/2007 Last Review/Update: 04/01/2011

Approved: 04/05/2011 Signed: ______________________________