

- ❖ **Policy Title** - Firewall Management
- ❖ **Policy ID** - TSD-1002
- ❖ **Version** - Version: 1.0
- ❖ **Supersedes** – Not applicable. This is the first version.
- ❖ **Review Date** – One (1) year from effective date.
- ❖ **Procedures** - Device Installation Guidelines, Network Configuration Management
- ❖ **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.
 - Preinstallation
 - A system profile form for each system 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.
 - No new system may be deployed behind a NET-managed firewall before a system profile has been completed.
 - 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 hardcopy of administrative passwords for all firewalls shall be kept in the safe in the Thompson Data Center.
 - 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: 04/30/04 Last Update: ___/___/___

Approved: ___/___/___ Signed: _____