

- ❖ **Policy Title** - Change Management for Network Devices
- ❖ **Policy ID** - TSD-1001
- ❖ **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 describes a framework to be used for controlling software, hardware, and configuration changes made to equipment used in the University's enterprise data network.
- ❖ **Purpose** - Appropriate change management controls provide the following benefits:
  - Increase network availability and uptime by providing a database of baseline configuration information for each device that can be quickly restored when necessary
  - Ensure that required security measures are in place on all deployed equipment
  - Provide a communications vehicle to inform others in the organization when changes are made to key systems
- ❖ **Applicability** - Applies to all routers, switches, hubs, gateways, servers, and other active devices managed by Network Engineering and Technology (NET) and used as components in the University's production data network. *Note: This policy does not apply to cabling infrastructure, lab equipment, or devices used solely for test, monitoring, or management purposes.*
  - Initial Installation
    - When equipment is initially installed, it should be configured in accordance with NET operating procedures. Particular attention should be paid to access filters, passwords, and any security guidelines that pertain to that type of equipment.
    - The installer shall make an entry in the "Public" section of the NET Log application as soon as practical after the new system is put into service, describing the location, type, and purpose of the new unit Detailed technical information should be avoided, as this step is intended only to communicate the fact that a change was made to a particular area or function at a given time, by the named individual. This information is then forwarded to the TSD Change Management System and to the ITU Support

Center and departmental technical contacts as appropriate, using the pulldown menu in the NET Log application. An example of a "Public" log entry might be:

Added second router chassis to MESA Network Enterprise Core for redundancy.

- The installer must record pertinent information such as IP address, physical location, and any other pertinent details in the "Private" section of the NET Log, for reference by NET personnel.
- The device's configuration file, if one exists, must be saved in accordance with NET operating procedures.
- Existing component-level network drawings shall be updated as soon as possible to indicate the location and address of the new device.

### ❖ Configuration Changes

- Changes that must be logged include hardware replacement, software updates, filter/ACL changes, modifications to uplinks, device resets or anything else that could affect the basic functionality of the device. Anyone making such a change must follow the steps listed in 1.a-e above.
- Actions that are unlikely to affect the device's basic functionality do not have to be logged. Examples: mirroring a port, adding or removing a patch cable for an access port. If any doubt exists, even a minor change should be logged.

### ❖ Compliance

All Network Engineering and Technology personnel have a responsibility to comply with this policy.

Effective Date: 04/30/04    Last Update: \_\_\_/\_\_\_/\_\_\_

Approved: \_\_\_/\_\_\_/\_\_\_      Signed: \_\_\_\_\_