POLICY NAME: Change Management (CM) for Network Devices Policy

Effective Date:	The policy will become effective as of the date of approval.
Policy Owner:	Network Engineering & Technology, TSD
Policy Number:	TSD-1001
Related Policies:	CM for Hardware/Software Supporting ITU Services Policy
Purpose:	The purpose of this policy is to describe a framework to be used for controlling software, hardware, and configuration changes made to equipment used in the University's enterprise data network. 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
Scope:	Change Management (CM) for Network Devices Policy 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.
Policy Statement:	This policy defines the roles and responsibilities of the Network Engineering and Technology (NET) unit and the university

	community with respect to controlling software, hardware, and configuration changes made to equipment used in the University's enterprise data network planning.
Definitions:	None
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 configuration of routers, switches, hubs, gateways, servers, and other active network devices.
Compliance:	All university employees, contractors, and business partners and all Network Engineering and Technology personnel responsible for initial installation and/or changes to network configuration shall comply with this policy. System owners must have documented Configuration Management procedures for network device 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 when required for auditing purposes. Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action.
Implementation Process:	Information concerning initial installation configuration and changes to configuration of network devices shall be maintained in the TSD Change Management Database. Network devices include: • Any device which directly supports enterprise applications or services, such as a PBX system or any equipment located in the Network Enterprise Core

- Any device acting as a router or aggregation switch for one or more buildings
- Any device acting as a firewall, VPN gateway, or other unit whose primary purpose is to control access to the university's administrative systems

Initial Installation

- Installations or configuration changes to equipment listed above must be authorized and documented in accordance with TSD Change Management guidelines, with device descriptions entered into the TSD CM Database.
- 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 optionally may make an entry in the "Public" section of the NET Log application 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. The Public log information is then forwarded 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 NET Log is not a substitute for the TSD CM database, but may be used to record supplemental information or to record changes to equipment not required to be maintained in the CM database (for example, access switches.)
- 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.
- Device replacements and configuration changes that will affect the basic functionality of the equipment entered into the TSD CM Database must be either preauthorized (in non-emergency situations) or entered after the work is completed with the designation “Emergency” or “Late” in accordance with TSD CM procedures.
- 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.

Approved By:	Walt Sevon Deputy CIO Executive Director, Technology Systems division
Approval Date:	July 31, 2007
Revision History:	*N/A*
Supersedes (Previous Policy):	*N/A*
Date of Review:	*Reviewed April 5, 2011*

Policy Contact Name:

Policy Contact E-mail: