**POLICY NAME:** Change Management (CM) for Hardware/Software Supporting ITU Services Policy

**Effective Date:** June 30, 2006

**Policy Owner:** Technology Systems Division

**Policy Number:** TSD-1004

**Related Policies:** Change Management (CM) for Network Devices (TSD-1001)

**Purpose:** Establish change management (CM) policy to control software, hardware and configuration changes made to assets.

**Scope:** This policy applies to all TSD departments (or the ITU) and all assets owned and maintained by the university for which one or more production ITU services are, or will be, dependent. An asset must be under CM control if removal or misconfiguration of the asset may cause diminished capacity or outright service fault of an ITU-managed service. This includes assets that are being configured in anticipation of being in production.

This policy does not apply to cabling infrastructure, lab equipment, or hardware/software/devices used solely for test, monitoring, or management purposes.

**Policy Statement:** This policy defines the roles and responsibilities of the Information Technology Unit or (TSD) with respect to establishing change management controls to increase service availability and uptime, to ensure that required security measures are in place on all deployed hardware/software and to provide a communications vehicle to inform others in the organization when changes are made to key systems.
Definitions:

Asset: hardware and software resources

Change Management System: A System to track initial configuration of hardware and software and changes to that configuration over time

CRB: Change Review Board

CM: Change Management

Responsibilities:

The Change Review Board (CRB) is responsible for:

- Review and consent for changes processed through the Change Management system
- Oversight over scope as defined above, and as further specified by participating departments, including defined types of changes applicable to CM-controlled assets
- Compliance monitoring

The following TSD departments will provide initial membership to the CRB:

- Database Application Services (DAS)
- Enterprise Servers & Messaging (ESM)
- Network Engineering & Technology (NET)

It is recognized that not all changes require the CM process. It is the responsibility of area managers to define local policies to further refine the assets and types of changes that must be under CM control, and the types of changes that are exempt from CM control. The Change Review Board must grant exemption from CM for changes to assets above.

Compliance:

All TSD Departments are required to abide by this policy. All changes to assets within the scope of this policy must be processed through the change management system defined at http://cmdb.gmu.edu. All assets within the scope of this policy
must be defined and maintained in the ITU change management database, located at http://cmdb.gmu.edu.

The Change Review Board shall report instances of noncompliance to the Executive Director, Technology Systems Division.

Implementation Process: Change management controls will be established by the Change Review Board (CRB). The CRB will create a process by which changes to CM-controlled assets are monitored and communicated to appropriate personnel. The objectives of the CRB are to ensure applicable system changes receive:

- Peer review
- Informed Consent
- Better planning and coordination
- Reduced error
- Reduced Time to Recovery

Also, in order to increase service availability and uptime, a database of baseline configuration information will be created for each asset that can be quickly restored when necessary.

Approved By: Walt Sevon
Deputy CIO
Executive Director, Technology Systems division

Approval Date: January 18, 2011

Revision History: N/A. This is Version 1.1

Supersedes (Previous Policy): N/A. This is the first version.

Date of Review: Reviewed January 18, 2011
Policy Contact Name:

Policy Contact E-mail: