POLICY NAME:  Operational Monitoring for ITU Services Policy

Effective Date:  April 15, 2008

Policy Owner:  ITU Technology Systems Division

Policy Number:  TSD-1005

Related Policies:  Configuration Management for Hardware/Software Supporting ITU Services Policy

Purpose:  The purpose of this policy is to institute practices to protect continuity of operations by monitoring the operational state of production services and supporting hardware.

Scope:  This policy applies to all services deemed critical to university operations, and the hardware that supports those services. Critical services are those services that represent a strategic, legal, financial or safety risk if left in a state of diminished performance or complete service fault. Critical hardware is the hardware which if operating outside of normal parameters could cause a critical service to enter a state of diminished performance or complete service fault.

Note: 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 establishes a requirement for operational monitoring of production services and supporting hardware.

Definitions:  None.

Responsibilities:  The Commonwealth of Virginia has published policies and
minimum standards to be followed by all state agencies for operational monitoring. Responsibility for operational monitoring of ITU 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 operational monitoring.

Compliance: All TSD Departments are required to abide by this policy. Asset administrators shall perform annual reviews of existing monitors to ensure completeness and accuracy of monitoring methods. Any changes, modifications, or revisions to policies related to the governance of the university’s Information Technology Infrastructure, Architecture, and Ongoing Operations will be reviewed in light of the latest versions of the standards and guidelines upon which these key components are based. Any changes, modifications, or revisions to systems dependent upon the university’s Information Technology Infrastructure, Architecture, and Ongoing Operations will be required to be compatible with the published standards and guidelines. Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action.

Implementation Process: All assets within the scope of this policy must be monitored with an ITU approved monitoring tool. New assets within the scope of this policy must be monitored before going into production. The asset administrator shall work with the monitor administrator to establish reasonable monitoring methods to ensure detection of service outages and to the extent possible, diminished performance.

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

Approval Date: January 18, 2011

Revision History: N/A

Supersedes (Previous Policy): N/A

Date of Review: January 18, 2011

Policy Contact Name:

Policy Contact E-mail: