**POLICY NAME:** Logging for Equipment Supporting ITU Services Policy

**Effective Date:** The policy will become effective as of the date of approval.

**Policy Owner:** Technology Systems Division

**Policy Number:** TSD-1007

**Related Policies:** TSD Logging Standards Document

**Purpose:** Logging is a necessary measure for identifying, responding to and preventing events such as operational problems, security incidents, policy violations, performance issues and fraudulent activity. This policy ensures that logs generated by IT assets are reviewed for these and other events that could have a deleterious effect on continuity of operations or on the university as a whole.

**Scope:** This policy applies to TSD servers, network devices, hosted services and software applications therein.

**Policy Statement:** All assets within the scope of this policy must conform to the TSD Logging Standards Document. (note: this document is not found online) While exceptions to this policy weaken security posture, it is recognized that some exceptions may be necessary. The IT Security Officer or his/her designee shall approve or deny all requests for exceptions.

**Definitions:**

- **Logging:** Logging is an automatically generated audit trail of access information.

**Responsibilities:** The Commonwealth of Virginia has published policies and minimum standards to be followed by all state agencies during
the installation of data and voice communications networks.
Responsibility for logging of equipment supporting the
Information Technology Unit at all campuses of George Mason
University resides with the Vice President for Information
Technology. The Technology Systems Division, under the
direction of the Vice President for Information Technology, is
responsible for setting local standards and policies for logging.

Compliance:
All TSD Departments are required to abide by this policy.
Management or other designated individuals are responsible for
ensuring appropriate compliance with this policy within their
area of responsibility.

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: Mason shall, or shall require that its service provider, document
and implement information security monitoring and logging
practices that include the following components, at a minimum:
Information Security Standard COV ITRM Standard SEC501-01
Date: August 11, 2009 (Revision 5) 42
1. Designate individuals responsible for the development and
implementation of information security logging capabilities, as
well as detailed procedures for reviewing and administering the
logs.
2. Enable event logging on all IT systems. At a minimum, logs will
include:

a. The event;
b. The user ID associated with the event; and
c. The time the event occurred

Note: Examples of events might include logons, invalid access attempts or data deleted, changed or added.

3. Routinely monitor IT system event logs, correlate information with other automated tools, identify suspicious activities, and provide alert notifications.

4. Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.

Example: Possible actions include stopping the event, shutting down the IT system, and alerting appropriate staff.

Note: Multiple actions may be warranted and advisable, based on sensitivity and risk.

5. Prohibit the installation or use of unauthorized monitoring devices.

6. Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.

Note: For investigative purposes, the Chief Information Security Officer (CISO) or Information Security Officer (ISO) has the responsibility to authorize monitoring or scanning activities for network traffic; application and information access; user commands; email and Internet usage; and message and information content for IT systems and data.