



OIT 62.903: Information Security Monitoring and Logging

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Information Security Monitoring and Logging addresses protection of IT systems and information by implementing and reviewing security monitoring and logging.

II. Purpose

The Information Security Monitoring and Logging policy identify the steps necessary to monitor and record IT system activity.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

The University 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:

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 CISO or 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.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate Vice President or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.