Purpose:
To provide accurate and comprehensive audit logs in order to detect and react to inappropriate access to, or use of, information systems or data.

Scope:
This policy applies to all Information Systems that store, process or transmit University Data.

Policy:
1. Access to Information Systems and data, as well as significant system events, must be logged by the Information System.

2. Information System audit logs must be protected from unauthorized access or modification.

3. Information System audit logs must be retained for an appropriate period of time, based on the Document Retention Schedule and business requirements. Audit logs that have exceeded this retention period should be destroyed according to UF document destruction policy.

Responsibilities:
1. Information System Administrators (ISAs) are responsible for developing and implementing procedures for the reporting and handling of inappropriate or unusual activity.

2. Information System Managers (ISMs) are responsible for monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity.

Authority:
UF-1.0102: Policies on Information Technology and Security
Policy: Information Technology Audit and Logging

References:

NIST 800-53r3: AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-10, AU-11, AU-12

University of Florida General Records Schedule: http://cms.uflib.ufl.edu/records/Schedules