UF UNIVERSITY of FLORIDA Health Science Center

Security Program for the Information and Computing Environment

POLICY

Policy: TS0003	Category: Technical Security	Version Date: 9/14/2004
Title: Logging & Information System Activity Review - Electronic Information		Effective Date: 3/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review:
Review Resp: HSC Chief, Information Security		Next Review:

Purpose:

To establish policies for logging/information system activity review involving electronic information assets.

Scope:

This policy applies to all UF HSC Units and individuals including, but not limited to, UF HSC faculty and staff, volunteers, students, and third parties.

References:

1. Standard TS0001: Logging/Information System Activity Review and Review Documentation
2. UF Information Technology Security Policy - http://www.it.ufl.edu/policies/security/index.html

Policy:

1. All network access activity must be logged according to the UF Information Technology Security Policy - Authentication, Authorization, and Auditability section. These logs must be securely maintained for the appropriate time per the UF IT Security Policy.
2. All other information system activity may be logged at the discretion of the Unit Information Security Administrator, the Unit Information Security Manager, and the owner's designee or delegate responsible for the information.
3. All electronic logs must be accurately time stamped.
4. Access to and confidentiality of logs must be strictly controlled.
5. The following must not be logged:
   a. Passwords;
   b. Data retrieved via informational application queries (e.g., reports, displays). Note: the activity of executing a query may be logged.