UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: TS0003.02	Category: Technical Security	Version Date: 9/14/2004
Title: Logging/Information System Review Activity and Review Documentation		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 delineate guidelines for logging/information system review activity and documenting reviews involving electronic information.

Reference:

1. Policy TS0003: Logging & Information System Activity Review - Electronic Information

Standard:

1. Logs/Information System Activity Reviews shall be reviewed periodically at the discretion of the Unit Information Security Administrator in conjunction with the owner's designee or delegate of the data. The reviews must be documented and the documentation kept for six years. Documentation of activity involving electronic information must include:
   a. The date of the review;
   b. The person or persons conducting the review;
   c. The information/data involved;
   d. The results of the review;
   e. The disposition of any activity that required investigation.

Guidelines:

1. In addition to the logging requirements in the UF IT Security Policy, it is recommended that the following items be logged:
   a. System activity associated with all system administrators
   b. Significant security events involving UFHSC computer systems that handle Restricted and Sensitive data. Examples of significant security events include obtaining and viewing of electronic patient health information, password-guessing attempts, attempts to use privileges that have not been authorized, modifications to system or application software, and changes to user groups or accounts.
   c. Key user activity information involving computer applications that support processing of Restricted and Sensitive data:

i. User session activity including user-IDs, log-in date/time, log-out date/time and applications invoked
ii. Changes to key application system files
iii. Additions and changes to the privileges of users
iv. System start-ups and shut-downs

2. The logs mentioned above should be kept at a minimum of one year. The exact length of time over one year will be set at the discretion of the Unit Information Security Administrator in conjunction with the owner's designee or delegate of the data.