

**MICHIGAN STATE UNIVERSITY
HEALTH INFORMATION TECHNOLOGY
POLICIES/PROCEDURES**

SUBJECT:	Server Log Retention for Servers with Sensitive data	NO: IS - 15
SCOPE:	Health Information Technology Network Support Staff	Page 1 of 1
AUTHOR:	JJ Strieff, Linda Losik	INITIAL REVIEW REQUIRED BY:
FINAL APPROVAL: Jerry Aubert, CIO		
EFFECTIVE DATE: 10/2007		REVIEW DATE: 10/2008
KEYWORDS:		

POLICY STATEMENT

All Health Information Technology (HIT) servers that contain sensitive data as defined by Federal laws such as HIPAA, FERPA, or State of Michigan law such as Act Number 556, (<http://www.legislature.mi.gov/documents/2005-2006/publicact/pdf/2006-PA-0566.pdf>), or industry standards such as PCI DSS will retain logs for seven years.

PROCEDURE

HIT Network Support Staff

Security Officer and Network Manager

1. Log files shall be increased to a reasonable size text file without automatic overwriting.
2. Logs are not required to be stored on the server as long as the file can be accessed.
3. All log files shall be included in the daily tape backup.
4. After 30 days, logs files can be copied to another form of electronic storage.
5. If the logs appear to be tampered or altered, the Security Officer should be notified by the Network Manager.
6. The Security Officer will document all actions and maintain records for seven years.