SYSTEM LOG FILES

RECORDS RETENTION SCHEDULE

CREATED JULY 2015

MICHIGAN STATE UNIVERSITY

MICHIGAN STATE UNIVERSITY SYSTEM LOG FILES RECORDS RETENTION SCHEDULE:

University Archives and Historical Collections has developed this retention schedule to document the nature of system records created by the university and define the appropriate retention period according to the legal, fiscal, administrative, and historical needs of the university.

The System Log Files Records Retention Schedule applies to all system documentation at Michigan State University, regardless of format or media. For additional information regarding electronic records management, please go to the University Archives website at http://archives.msu.edu/.

Not all offices may create all the record series listed on the retention schedule. If you are not currently creating records in a series, you do **NOT** need to start creating new records.

If you believe that you have a record that does not fall under a specific record series, please contact University Archives at 5-2330. University Archives will either help you identify which record series applies to your record or will create a new record series. Do not assume that the record can be destroyed; all records reflecting the official activities of university officers and offices are the property of Michigan State University and thus cannot be destroyed without the approval of the director of the Archives.

Please note that all records pertaining to ongoing or pending audits, lawsuits or even reasonably anticipated lawsuits, and public disclosure proceedings may not be destroyed, damaged, or altered until the issue is resolved, and an office or unit has been specifically advised that such records may be destroyed. Any of these conditions supersedes the retention period listed in the records retention schedule.

NON-RECORDS:

According to State of Michigan guidelines, some records used at Michigan State University can be considered non-records. These non-records are not covered by the retention schedule and may be destroyed once they are no longer administratively necessary.

Non-records may include:

- Duplicate copies of documents retained for distribution or convenience
- Miscellaneous notices of memoranda such as “All-Staff” emails, messages on upcoming events, or memos on minor administrative details
- Blank forms
- Unsolicited advertising and product catalogs
- Preliminary drafts of letters, memoranda or reports that do not form significant stages in the preparation of a final document
- Personal messages or correspondence
- Non-university publications, such as manuals, directories, catalogs, newsletters, pamphlets, and periodicals

Please contact University Archives at 517-355-2330 or at archives@msu.edu with any questions regarding non-records.

DESCRIPTION OF TERMS:

Schedule Title: This is the official title of the individual record series.

Schedule Description: This is the official description of the individual record series, usually consisting of a general statement of record function, followed by a description of some of the documents that can be found in that record series.

Schedule Retention: This is the minimum amount of time that the record series must be kept, also known as a retention period. It typically consists of a retention code plus a date range in years.

For example) Schedule Retention: CR+0/3 (Creation Date + 3 months/90 days)

The retention code index can be found below.

Retention Code Index:

Retention Code	Retention Period Description
CR	Creation Date

Event Date: This documents the event after which the retention period will be applied. Some retention periods can be applied only after a specific event or date has occurred. For example, access logs must be retained for 90 days from the date of creation. Thus, the creation date is the event date from which the retention period is measured.

Disposition: This is a statement that describes how long the document must be kept and how it must be destroyed. Many university records contain confidential information, such as social security numbers; thus, University Archives recommends confidential destruction, i.e. shredding, whenever possible to protect personal information.

Office of Record: This field identifies the office that is responsible for maintaining the official record series. The designated office keeps the record for the entire retention period and then arranges for its destruction once the retention period has passed. Other offices which maintain copies of a record series but are not the office of record may destroy those non-records when they are no longer administratively necessary unless otherwise noted in the schedule.

Notes: This may document additional notes about the retention series, legal citations affecting retention, or university best practices regarding the records.

SPECIAL NOTE ON SYSTEM LOG FILES:

Due to the size of system log files, offices should prioritize storage of critical system files over storage of non-critical system files. For questions regarding critical systems, please contact MSU Information Security at informationsecurity@msu.edu .

ADDITIONAL GUIDANCE:

For any questions, concerns, or additional guidance regarding this retention schedule, please contact University Archives at 517-355-2330 or at archives@msu.edu .

Schedule Approved: 12/1/15

Michigan State University

Information Technology Records

Schedule Title	System Log Files, Access Logs
Schedule Description	This record series documents the events and actions taken in university information technology systems in regard to system access. These log files may include, but are not limited to: application logs, authentication logs, database logs, email logs, firewall logs, physical security (key/video) logs, syslogs/event logs from servers, VPN logs, and web server logs. These logs may be found in the following systems: AD, LDAP, Radius, Shibboleth, Kerberos, SQL, Oracle, Exchange, Sendmail, Anti-SPAM, SSL VPN, IPSec, Apache, IIS, and Tomcat as well as other systems not listed here.
Schedule Retention	CR+0/3
Event Date	Creation
Disposition	Retain for at least 90 days after records creation, but for no longer than 1 year, then purge from system.
Office of Record	IT Services and Department/Office IT Staff
Notes	Retention is based on federal guidelines, including 21 CFR Part 11. This record series does not address log files that are maintained in accordance with PCI-DSS, HIPPA, or Gramm-Leach Act requirements. Please consult appropriate regulatory documentation for further details on retaining those log files. Due to the size of system log files, offices should prioritize storage of critical system files over storage of non-critical system files. For questions regarding critical systems, please contact MSU Information Security.

Schedule Title	System Log Files, Network Logs
Schedule Description	This record series documents the events and actions taken in university information technology systems in regard to network procedures. These log files may include, but are not limited to: ARP cache date, bandwidth statistics for internal and external links, DHCP lease logs, DNS query logs, NAT logs, router/switch logs, and wireless controller logs.
Schedule Retention	CR+0/1
Event Date	Creation
Disposition	Retain for at least 30 days after records creation, but for no longer than 1 year, then purge from system.
Office of Record	IT Services; Deparment/Office IT Staff
Notes	Retention is based on federal guidelines, including 21 CFR Part 11. Bandwidth statistics may have permanent retention due to historical value. This record series does not address log files that are maintained in accordance with PCI-DSS, HIPPA, or Gramm-Leach Act requirements. Please consult appropriate regulatory documentation for further details on retaining those log files. Due to the size of system log files, offices should prioritize storage of critical system files over storage of non-critical system files. For questions regarding critical systems, please contact MSU Information Security.

Schedule Title	System Log Files, Security Logs
Schedule Description	This record series documents the events and actions taken in university information technology systems in regard to information security. These logs files may include, but are not limited to: anti-virus logs, IDS alert data, incident records, and packet captures (TCPdump).
Schedule Retention	CR+0/2
Event Date	Creation
Disposition	Retain for at least 60 days after records creation, but for no longer than 1 year, then purge from system.
Office of Record	IT Services; Department/Office IT Staff
Notes	Retention is based on federal guidelines, including 21 CFR Part 11. Some alert data statistics may have permanent retention due to historical value. If incident reports/captures are ongoing or currently active, logs must be retained until the incident is closed. This record series does not address log files that are maintained in accordance with PCI-DSS, HIPPA, or Gramm-Leach Act requirements. Please consult appropriate regulatory documentation for further details on retaining those log files. Due to the size of system log files, offices should prioritize storage of critical system files over storage of non-critical system files. For questions regarding critical systems, please contact MSU Information Security.