Log Management

I. INTRODUCTION

This policy establishes a log management expectation for managing computer and system logs, as the Information Security policy requires. Most computer systems produce system logs that capture events that have occurred within a system or network. Logs are needed when performing auditing and forensic analysis to support internal investigations, establish baselines, and identify operational trends and long-term problems.

II. POLICY OVERVIEW

The purpose of this policy is to set requirements and goals for the generation, transmission, storage, analysis, and disposal of computer system logs. At a high-level log management includes:

- Establish policies and standards for log management.
- Assign responsibility for managing and maintaining organization’s computer logs.
- Create and maintain a log management infrastructure.
- Establish standards for log management operational processes.

System log files provide the ability to support for:

- Suspicious and malicious activity detection and monitoring
- System performance monitoring
- Forensic analysis and investigation
- System and network troubleshooting

III. POLICY PROCESS

A. Requirements

1. University-owned, leased, or operated systems shall, at a minimum and whenever possible, be capable of and configured to:

    a. Produce event logs with the minimum necessary event information – see #6

    b. Synchronize their time with the University's common time source.

2. University-owned system must be able to produce event logs in a widely used format such as JSON, Windows Event Logs, Common Event Format, Common Log Format, etc.

3. At a minimum, University-owned systems must be able to use standard message logging protocols such as Syslog to send event logs to a centralized logging system.

4. The University will maintain a centralized log management system to capture and aggregate event logs.

5. Logging data shall be classified as Confidential and protected from unauthorized access, modification, and deletion.

6. At a minimum, log files should contain the following elements:

    a. Date, times, and details of events key to the operation of the resource

b. User IDs or other identification mechanisms

c. Success/failure of system access attempts

d. Source and target network addresses and protocols details

e. Action that occurred.

7. The University shall retain event logs for 3 years with at least 3 months available for 'online' access or as required by federal, state, or local laws and organizational policies.

8. Logging data shall be routinely reviewed and analyzed by trained personnel. The frequency and nature of log monitoring and review depend on the risks to the relevant computer system and underlying data. They shall be commensurate with a particular system's profiled data classification category.

   f. All security events and operational logs shall be reviewed to detect deviations from policy and to test the effectiveness of access control and security mechanisms.

   g. Review all events to detect unusual activity and suspicious events.

   h. Review all application and system events to discover errors and performance issues.

9. The log management system and logging data shall be protected against unauthorized tampering, modification, and destruction. Access to log files and logging data shall be audited, monitored, and restricted to need-to-know personnel.

10. Once logging data has reached the retention schedule, it shall be securely purged and eliminated unless it needs to be retained for legal or eDiscovery purposes.

11. IT Security personnel shall monitor log management processes and systems and conduct audits, at least quarterly, of the log management system.

B. Roles and Responsibilities

1. The Information Security Office (InfoSec) is responsible for protecting the log management system, monitoring activity logs, and auditing the log management system.

IV. DEFINITIONS

- **Log** – a file that stores a record of the events that occur in a computer system.
- **Logging Data** – information contained within log files.