UDAD Policy 925.1
Division Information Technology Security:
Audit Logging and Monitoring Policy

Purpose
To provide accurate and comprehensive audit logs to detect and react to inappropriate access to, or use of, information systems or data.

Scope
This policy applies to all Information Systems that store, process, or transmit the University of Arkansas System, Division of Agriculture (UADA) data. Microsoft InTune maintains, monitors, and analyzes security audit logs for covered devices.

Policy
1. Access to Information Systems and data, as well as significant system events, must be logged by the Information System.
2. Information System audit logs must be protected from unauthorized access or modification.
3. Information System audit logs must be retained for an appropriate period of time, based on the Document Retention Schedule and business requirements. Audit logs that have exceeded this retention period should be destroyed according to UADA Data Retention and Disposal Policy.

Responsibilities
1. Information System Administrators (ISAs) are responsible for developing and implementing procedures for the reporting and handling of inappropriate or unusual activity.
2. Information System Managers (ISMs) are responsible for monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity.

Accountability and Contacts
The Chief Information Officer for UADA is charged with the responsibility to periodically review the policy and propose changes as needed.

Reference Documents
Data Lifecycle and Management Policy and Procedures (UADA Policy 920.1)