INFORMATION SECURITY STANDARD

Effective Date: July 11, 2018
Last Revised: August 19, 2022

AUDITING, LOGGING, AND MONITORING

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or *Data Classification and Handling* policy. Questions regarding the *Information Security Standards* should be directed to Information Security Services.

This Information Security Standard establishes minimum logging and monitoring requirements for University IT R

Microsoft Windows Event Logs, Microsoft Active Directory logging, Microsoft Azure Log Analytics

Microsoft Advanced Threat Protection – tools that provide automated monitoring and alerting for anomalous user and system activities on the domain

Logging via syslog, syslog-ng, and other similar formats from non-Microsoft systems and network appliances

Application logging to files or databases

Database logging, such as Oracle and SQL

4.1. Information Security Services will assist with implementation of universal forwarders to provide for log collection into a central correlation application.

4.2. In all cases, regardless of storage location (on the IT Resource itself or forwarded to a central application), logs should be protected from unauthorized access, modification, and deletion. Specific access controls are outside of the scope of this standard, but all access to logs shall be controlled in accordance with the University's *Access Control* policies and *Data Handling Protocols*.

5. Retention and Review. Logs should be retained according to University Records retention policies and for no less than two weeks. Periodic reviews of security event logs, logs from critical systems performing security functions, or those identified in section 3 should be performed as necessary to identify anomalous activity. Alerts should be configured to automate the review and detection of anomalous and high-risk activities and delivered to system administrators, system owners, data owners, and/or security analysts for potential incident identification and classification. The following events should be reviewed frequently or configured with alerting when possible.

Events identified as information security incidents (as described in the *Information Technology Incident Management* policy)

Logs of systems that store, process, or transmit Sensitive and/or Highly Sensitive Information

Logs of systems identified in section 3 above

Logs of servers and systems that serve as firewalls, intrusion-detection systems, authentication servers, and financial transaction systems