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 Resources. Logging is an essential IT function that is used to identify, respond to, and prevent incidents, policy violations, fraudulent activity, operational problems, system errors, or performance events, as well as to comply with applicable auditing requirements and laws and regulations.

1. **Scope**. All University IT Resources, especially those that transmit or store Sensitive and/or Highly Sensitive Information, provide network connections, or function as part of authentication, authorization, or access control systems, shall be configured to record appropriate auditing and logging information.

2. **Logged Activities**. At a minimum, the following activities shall be logged:
   2.1. Authentication, Authorization, and Accounting:

   - Create, read, update, or delete Sensitive and/or Highly Sensitive Information, including authentication information such as passwords
   - ~~A network connection is accepted or blocked~~
   - User authentication and authorization, including login and logout
   - Granting, revoking, or modifying access rights, including the addition of a new user or group, user password changes, the changing of permission/privilege levels, file permissions, database object permissions, or firewall rule sets
   - 2.2 Endpoint Configuration and Patching:
   - Installation of software patches and updates or other configuration changes
   - 2.3 Endpoint Security and Activity:
   - Application and system software process startup and, when possible, shutdown or restart
   - Detection of suspicious or malicious activity such as anti-virus software detections and, where possible, network activities detected by intrusion detection systems or firewalls
   - A network connection is accepted or blocked
   -

3. **Log Elements**. At a minimum, activity logs shall contain the following elements:

   - Type of action – such as authorize, create, read, update, delete, accept, deny, block
   - What is performing the action – such as subsystem, process, service, transaction, application
   - Who is performing the action – such as username or user ID, computer or hostname, IP address, mac address, service or process name
   - What object had an action performed on it – such as file name accessed, record accessed in a database, query parameters used, computer or hostname, IP address, user ID
   - Date and time the action was performed
   - Outcome of the action – such as allowed, denied, success, failure, error code
     - If applicable, description or event/reason code for failure or denial

4. **Formatting and Storage**. IT Resources differ by operating system, role, and function. This results in varying log formats. Additionally, log forwarding to a central collection system capable of translating disparate formats for correlation should be used where appropriate. Some methods for logging and log collection that are approved and widely deployed at Northern Arizona University include:

   - Microsoft Windows Event Logs, Microsoft Active Directory logging, Microsoft Azure Log Analytics
   - Microsoft 365 Defender – 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 agents to provide log collection into a central storage, monitoring, and 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.~~ 5. **Retention and Review**. Logs should be retained according to University Records retention policies and for no less than two weeks where possible. Logs identified in section 2.3 should be retained for thirty days where possible. Regulations and logs specific to certain system must be abided by when longer retention is required.

~~-~~Periodic and automated reviews of security event logs, logs from critical systems performing security functions, or those identified in section 2.~~3~~ should be performed as necessary to identify anomalous activity.

Alerts should be ~~configured~~ defined by system, service, and/or D~~d~~ata ~~owners~~ Stewards to automate the ~~review and detection~~reporting 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~~response. ~~The following~~All ~~events~~ logs identified in section 2 should ~~be reviewed frequently or configured with~~ have such alerting created when possible or be reviewed manually on a monthly basis.

~~- 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~~