Cochise County
Board of Supervisors

Public Programs...Personal Service
www.cochise.az.gov

Policy Title: Audit and Accountability

Policy Number: 1803

Effective: June 1, 2019

Supersedes:

Last Reviewed/Updated:

Scope/Coverage: All Information Technology (IT) Resources owned or operated by Cochise County

Policy Contact: IT Department

Source Document Reference: Policy reflects standards of the National Vulnerability Database (NVD). Content contains hyperlinks to NVD sources. The NVD is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division.

I. Audit Events (AU-2)

CCIT will determine the information systems capability of auditing the required events (i.e., logon, logoff, password changes, and administrative group changes) and will document any exceptions. Information systems are configured to capture Notice level alerts and higher. If a system requires a less detailed level of audit CCIT will document the level and rational why the auditable events are deemed to be adequate.

II. Content and Audit Records (AU-3)

Whenever possible audit records captured will include information establishing the type of event, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

III. Audit Storage Capacity (AU-4)

CCIT will ensure that sufficient audit record storage capacity is available to maintain the audit records in accordance with applicable data retention guidelines and will not be accessible by personnel with Administrative permissions.

IV. Response to Audit Processing Failures (AU-5)

In the event of an audit processing failure, the default standard is to overwrite the older audit files but may be changed based on the criticality and capability of each system.

V. Audit Review, Analysis, and Reporting (AU-6)

CCIT will review and analyze information system audit records at least monthly for indications of inappropriate or unusual activity and report findings to the Chief Information Officer (CIO) or, if appropriate, to the County Administrator.