Cochise County
Board of Supervisors

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

Policy Title: Information Technology Access Control

Policy Number: 1801

Effective: July 1, 2022

Supersedes: June 1, 2019

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 reference to NVD sources in parentheses. 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. Account Management (AC-2)

A. CCIT will identify and select types of accounts, groups and role memberships as required to support the County's mission and business functions, and when applicable, approve account managers for specific information system (IS) accounts.

B. CCIT will authorize access to systems upon receipt of a valid **System Access Request Form** from department heads/elected officials or system account managers.

C. Department heads/elected officials, system account managers or human resources will notify CCIT immediately when users are terminated or transferred, accounts are no longer required, and if individual information system usage or need-to-know changes. Department heads/elected officials will ensure an **Employee Out-process Checklist** is completed.

D. County employee accounts will be verified every 2 years and non-county employee accounts will be verified annually to ensure the account is required and permissions are at the correct level for the individuals job duties.

E. Shared accounts will be reviewed and approved by the Cochise County Chief Information Officer (CIO) and only used when a dedicated account will not be adequate to accomplish the mission.

F. Shared account password will be changed every 90 days.

II. Access Enforcement (AC-3)

A. CCIT will use automated systems to enforce approved authorizations for logical access to information and system resources.

B. CCIT shall send an automatic notification to departments whenever IT accesses files or folders with restricted data.

C. The County Administrator has the authority to audit electronic file and folder access to ensure compliance with this requirement.

III. Information Flow Enforcement (AC-4)

CCIT configures information system to enforce logical separation when needed for the flow of information within the system and between interconnected systems.

IV. Separation of Duties (AC-5)

CCIT separates and documents the county defined duties of employees by dividing mission functions from support functions. The Information system defines access authorizations to support the separation of duties, ensuring data security personnel do not also administer data audit functions.

V. Least Privilege (AC-6)

Cochise County employs the principle of least privilege. Meaning, only authorized access for users (or processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with County mission and business functions.

VI. Unsuccessful Logon Attempts (AC-7)

Automated systems limit the number of consecutive invalid logon attempts by a user; the system automatically locks the account/node until released by an administrator or after a predefined period.

VII. System Use Notification (AC-8)

Information systems display to users a County defined notification message before granting access to the system. The message provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The message states.

> "You are attempting to access a Government information system; Information system usage may be monitored, recorded, and subject to public record requests and auditing; Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and Use of the information system indicates consent to monitoring and recording."

VIII. Previous Logon Notification (AC-9)

Information systems shall notify the user, upon successful logon to the system, of the date and time of the last logon.

IX. Session Termination (AC-12)

The information system automatically locks a user session after 15 minutes of inactivity. Any exceptions will be approved by the CIO.

X. Remote Access (AC-17)

CCIT establishes and documents usage restrictions for each type of remote access allowed.

XI. Wireless Access and Mobile Device access (AC-18, AC-19)

Cochise County restricts access to the operational wireless connection via directory login and permits open access to the guest wireless network. The operational and guest wireless network will maintain logical separation.

XII. Use of External Information Systems (AC-20)

Cochise County will establish terms and conditions with other organizations prior to permitting external connections to county-controlled networks or information systems.