Cochise County
Board of Supervisors

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

Policy Title: Configuration Management

Policy Number: 1804

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. Baseline Configuration (CM-2)

CCIT develops, documents, and maintains a current baseline configuration of all critical information systems (i.e. SolarWinds for network equipment, and Automate for Servers).

II. Configuration Change Control (CM-3)

A. CCIT determines the types of changes to the information system which are configuration-controlled, reviews proposed configuration-controlled changes and approves or disapproves such changes with explicit consideration for security impact analyses.

B. CCIT will use an automated system when possible to document configuration change decisions associated with the information system, implement approved configuration-controlled changes, and retain records of configuration-controlled changes for one year.

C. CCIT will audit and review activities associated with configuration-controlled changes.

D. Roll back process will be defined and documented in each configuration change request.

E. When time and cost permit the changes will be tested in a test environment prior to changing the operational environment.

III. Security Impact Analysis (CM-4)

CCIT will analyze changes to the information system to determine potential security impacts prior to change implementation.

IV. Access Restrictions for Change (CM-5)

CCIT defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

V. Configuration Settings (CM-6)

CCIT using security configurations reflecting the most restrictive mode consistent with operational requirements establishes and documents configuration settings for information technology. Identifies,

documents, and approves any deviations from established configuration settings based on operational requirements. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

VI. Least Functionality (CM-7)

CCIT configures the information system to provide only essential capabilities and where applicable, prohibits or restricts the use of functions, ports, protocols, and/or services.

VII. Information System Component Inventory (CM-8)

CCIT develops and documents an inventory of information systems within the Cochise County network enclave. CCIT will review and update the information system component inventory annually.

VIII. Configuration Management Plan. (CM-9)

CCIT develops, documents, and implements a configuration management plan for the Cochise County information systems. CCIT will be responsible for protecting the configuration management plan from unauthorized disclosure and modification.

IX. Software Usage Restriction (CM-10)

Cochise County uses software and associated documentation in accordance with contract agreements and copyright laws. CCIT tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution. Any use of peer-to-peer file sharing technology must be approved by the CIO and will be documented prior to implementation.

X. User-Installed Software (CM-11)

CCIT will use automated tools to scan information systems on the county network for unauthorized software and systems will be configured to prevent non-approved software.