Cochise County
Board of Supervisors

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

Policy Title: Contingency Planning

Policy Number: 1805

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. Contingency Plan (CP-2)

CCIT develops a contingency plan for the county information systems. CCIT will review the contingency plan every three years and update the plan to address changes as needed. CCIT will communicate contingency plan changes to relevant system owners and stakeholders and will protect the contingency plan from unauthorized disclosure and modification.

II. Contingency Training (CP-3)

CCIT will provide contingency training to information system users consistent with assigned roles and responsibilities based on the contingency plan.

III. Contingency Plan Testing (CP-4)

CCIT will test the contingency plan every three years to determine the effectiveness of the plan and the organizational readiness to execute the plan. CCIT will review the contingency plan test results and initiate corrective actions as needed.

IV. Alternate Storage and Processing Site (CP-6, CP-7, CP-8)

CCIT will establish an alternate processing site, network connectivity and storage site including necessary agreements to permit the storage and retrieval of information system backup information and ensure that the alternate site provides information security safeguards equivalent to that of the primary site. CCIT will ensure equipment and supplies required to transfer and resume operations are available at the alternate site or contracts are in place to support delivery to the site within 48 hours after major outage.

V. Information System Backup (CP-9)

CCIT conducts backups of enterprise level systems and does not maintain backups of end user desktops or laptops. Backups will include security-related documentation and will protect the confidentiality, integrity, and availability of backup information at storage locations.