



Cochise County Board of Supervisors

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

Policy Title: Information Technology Risk Assessment

Policy Number: 1808

Effective: July 1, 2022

Supersedes: June 1, 2019

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

Contact: IT Department

Source Document Reference: Policy reflects standards of the National Vulnerability Database (NVD), as referenced 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. Risk Assessment Policy (RA-1)

Cochise County will review and update the IT Risk Assessment policy and procedures annually, or more often as needed.

II. Security Categorization (RA-2)

Cochise County categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cochise County Data will fall within the following:

1. Restricted - Confidential information requiring the highest level of security and privacy protection. Access is only permitted as directed by the associated Data Steward or applicable authority.
2. Internal - Confidential information requiring diligent security and privacy protection. Information may be shared within the County on a need to know basis.
3. Public - Information may be published and shared freely.

III. Risk Assessment (RA-3)

CCIT shall conduct an annual risk assessment, including the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. This assessment shall include both internal and external penetration testing

IV. Vulnerability Scanning (RA-5)

Cochise County scans for vulnerabilities in the information system and hosted applications quarterly and when new vulnerabilities potentially affecting the system/applications are identified and reported.