# Cochise County
## Board of Supervisors

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

**Policy Title:** Acceptable Use

**Policy Number:** 1800

| | |
|---|---|
| **Effective:** | June 1, 2019 |
| **Supersedes:** | *Computer Usage & Accountability* |
| **Last Reviewed/Updated:** | |
| **Scope/Coverage:** | Cochise County Employees, and any users of County IT resources |
| **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. Responsible Network

A. Computer and network use shall be professional and business-like. All computer usage, software utilization and electronic communications, whether sent within the County or outside the County should withstand public scrutiny without embarrassment to the County, other employees, or the public.

B. Approved professional uses may include developing documents, cost accounting, communications with others for job related purposes using instant messaging technologies, and sharing or transferring data with other computers on the network, participation in professional associations, continuing education, scholarly publication, communications with colleagues, and subscription to distribution list servers, news groups or topical updating services related to Cochise County or a user's professional duties. Such use is subject to advance approval of the user's supervisor.

## II. Routine Use

A. Routine business uses include, but are not limited to, writing official correspondence, replying to official correspondence, scheduling meetings, request for information, the assignment of work tasks or clarification of assignments, conducting official research, notification of user's whereabouts, such as sick days or vacation requests, and the transfer of documents.

B. Limited personal use is permitted, subject to approval of the user's supervisor and in compliance with other sections of this policy. Personal use shall require minimal expenditure of workplace time and should be used in the context of lunchtime or break time. It is the responsibility of the user to ensure that the personal usage of the computing resource does not interfere with either their job performance, or the ability of others to use the resources.

## III. Prohibited Uses of The Computer Resources

A. Users may not use the PC, county network, telephones or Internet for commercial purposes or partisan political solicitations or uses that would otherwise violate County policies regarding employee time commitments or County equipment.

B. Users may not participate in any activity that might expose the county (i.e., create or forward chain letters), it's officials or the Information Technologies Department to liability resulting from the use of the equipment, network or Internet.

C. The County's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized content (i.e., copyrighted material).

D. Users shall not use the computer resources, network or Internet to intimidate or harass others, nor to interfere with the ability of others to conduct County business.

E. Users shall clearly identify themselves in any electronic communication, and shall not construct a document, or form of communication as to appear to be from anyone other than themselves.

F. Users may not use the computer resource, network or Internet to download software, unless they obtain prior permission from the Information Technology (IT) Department.

G. Users may not run or install software to any IT systems without the prior approval and coordination with the IT Department.

H. Users shall not attempt to gain unauthorized access to data, to breach or evade any security measures on the network, or to intercept any electronic communication without proper authorization from the IT Department.

I. Users shall not knowingly take any actions to bypass or circumvent security.

J. Users shall not use the computer resources or Internet access provided by Cochise County for connecting to, posting, viewing, or downloading pornographic, offensive, or other material that is inappropriate for the workplace or violates County equal employment opportunity or illegal discrimination and harassment policies.

## IV. Computer Resource Management

A. Appointing Authorities have the responsibility of ensuring electronic communications, information technology resources, and/or Internet access used by employees under his/her supervision are used to support activities connected with the business of Cochise County and follow policies and procedures outlined in this document and any other applicable Cochise County policies. The IT department monitors the use of all County IT systems and will provide reports to the Appointing Authority upon request. Additionally, the IT department reviews logs and will report extreme or repetitive misuse of computer resources to the responsible Appointing Authority and/or the County Administrator.

B. All personnel will review the Information Technology Use Policy prior to receiving access to any County Information Technology systems and re-read the policy on an annual basis.

C. All users must remain vigilant and inform the IT department of any suspicious emails or phone calls from someone trying to access their system.

## V. User Accounts and Passwords

A. All users have the responsibility to protect the County's computers, networks, and data from destruction, tampering, and unauthorized access. It is the responsibility of each user to establish appropriate passwords for their account and to change passwords periodically, to keep all passwords strictly confidential, and to prevent access by unauthorized individuals.

B. Each user shall access the County computer resource and network with his/her own user account and will not attempt to logon to the County computer resource or network by using the user account of another individual. In the absence of said user, IT Department personnel will assist other users who need to access information secured by another users account, with the approval from the CIO and the users Appointing Authority.

C. All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees will choose passwords that are at least twelve characters long and contain a combination of three of the following categories; upper- and lower-case letters, numbers, and special characters.

1. Employees must refrain from writing passwords down and keeping them at their workstations.

2. Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

3. Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT help desk (8301). Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be reported immediately.

## VI. County Access and Disclosure

A. Information Technologies will engage in the systematic monitoring of Internet access and the amount of time spent on the Internet by users.

B. Cochise County reserves the right to access and disclose the contents of electronic messages.

## VII. Public Access and Disclosure

A. All Electronic mail messages and files should be stored, preserved, and made retrievable according to law, policies, and procedures defining the public record status of the data. Materials in all categories can be released to the public if it is determined that the information is not exempt from disclosure.

## VIII. Policy Enforcement

A. When necessary to protect the security and integrity of the County Network, Information Technologies may disable network connections used by certain computers or users. This policy will be enforced by the CIO and/or County Administrator. Violations may result in removal of access to County information technology systems. Where illegal activities or theft of company property (physical or intellectual) are suspected, the County may report such activities to the applicable authorities.

B. Appointed Authorities, supervisors and users are expected to cooperate with any required investigation of possible violations of this policy.

C. When a violation of this policy is detected, the IT Department shall notify the appropriate Appointed Authority and Human Resources. The employees Appointed Authority is responsible for disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. The IT Department will remove access to any users that provide an unacceptable level of risk to the County network and will report to the County Administrator and Appointed Authority.

## IX. Accountability of Computing Resources

A. Each user that is assigned a mobile device (i.e., laptop computer, cell phone, tablet) will sign for their laptop and will be accountable for the security of the system when they remove it from the County complex. Laptops should not be left in the vehicle to help reduce the chances of theft. In the event of lost or stolen equipment the user needs to notify their supervisor and IT help desk immediately.