

Yuma County, Arizona

Information Security Policy

Control of Access to Information

The Information Technology Services department may control access to information maintained by Yuma County and the devices on which that information is stored, manipulated, and transmitted, in accordance with the laws of Arizona and the United States.

System Administration Access

The system administrator may access other's files for the maintenance of networks and computer and storage systems, such as to create backup copies of the media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

User Responsibility for Confidentiality of Information

Users are personally responsible for assisting in maintaining the security of any and all data to which they have access. The following items are specifically prohibited from disclosure:

Passwords – It is each employee's personal responsibility to guard the confidentiality of their passwords. No employee shall use any means to disclose their password with the exception of the disclosure of all passwords to a Yuma County Information Technology Services representative or designated Yuma County representative upon termination of employee's employment with Yuma County. There are no other exceptions.

Information – It is each employee's personal responsibility to guard the confidentiality of any confidential information they may gain access to during the performance of their duties for Yuma County. Confidential data or information is defined as any information not specifically designated as public.

Intellectual Property – Systems, processes, programs, and other intellectual property developed as part of the performance of any employee's duties and responsibilities during employment with Yuma County shall remain the sole intellectual property of Yuma County unless specifically designated as "open source" or granted release in writing by the County Administrator or Board of Supervisors.

Any user failing to comply with the stated policies regarding confidentiality of information shall be subject to disciplinary action that may include immediate termination.

Monitoring and Inspection

Users should also be aware that their uses of Yuma County computing resources are not private. While the Information Technology Services department does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance. Yuma County and the Information Technology Services department may also specifically monitor the activity, data and accounts of individual users of Yuma County computing resources, including individual login sessions and communications, without notice. This monitoring may occur in the following instances:

- The user has voluntarily made them accessible to the public.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of Yuma County from liability.
- There is reasonable cause to believe that the user has violated, or is violating, this policy.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- Upon receipt of a legally served directive of appropriate law enforcement agencies.

In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

Assessment and Analysis

Information Technology Services will perform periodic assessments and analyses in order to identify technology areas needing additional equipment or measures to adequately protect Yuma County computing and information resources. The benefits of such assessment and analysis include:

- Increasing security awareness at all levels of the organization.
- Evaluating the status of current policies and procedures of current security.
- Highlighting areas where greater security is needed.
- Gathering facts to reinforce policy and procedural guidelines.
- Justifying, prioritizing, and implementing effective counter-measures and procedures.

Security procedures

Information Technology Services has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, and to impose appropriate penalties when privacy is purposefully abridged.

Patches, Anti-Virus and E-mail Protection

Information Technology Services is responsible for maintaining and enhancing security on its network through the prompt deployment of software and security patches and providing anti-virus and e-mail protection. All computers and servers are protected through automatic or timely manual deployment of operating system patches and by the company's anti-virus program (Norton) and e-mail gateway.

Security Policy Users Access Review

Security policies and user access shall be reviewed on a yearly basis. Appropriate recommendations for changes in this policy will be submitted to the Yuma County Chief Information Officer for review by the Yuma County Board of Supervisors.