



Please return original document
to the **Board of Supervisors Office**,
ATTENTION: Ginger Hamilton, 928-373-1104
(Name & phone number)

TYPE OF DOCUMENT:

RESOLUTION NO. 2017-20

Adopt Resolution No. 2017-20, the Yuma County Information Security
Standards Policy and repealing
the Yuma County Computer Security Policy ID#0503 dated March 21, 2005.

DOCUMENT APPROVAL:

Approved by Yuma County Board of Supervisors:
July 17, 2017: Discussion Item No. 4.



YUMA COUNTY BOARD OF SUPERVISORS

RESOLUTION NO. 2017-20

ADOPTING THE YUMA COUNTY INFORMATION SECURITY STANDARDS POLICY AND REPEALING THE YUMA COUNTY COMPUTER SECURITY POLICY OF MARCH 21, 2005.

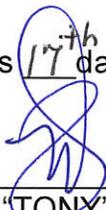
WHEREAS: Yuma County requests to establish minimum security standards throughout Yuma County and its business units to help ensure the confidentiality, integrity, security, and availability of Information Technology Resources (ITRs) so to be consistent with best practices associated with organizational information security management.

WHEREAS: Yuma County Information Security Standards Policy will replace the Yuma County Computer Security Policy ID#:0503 dated March 21, 2005.

WHEREAS: The Yuma County Board of Supervisors officially adopt the Yuma County Information Security Standards Policy.

NOW, THEREFORE, BE IT RESOLVED, THE YUMA COUNTY BOARD OF SUPERVISORS HEREBY ADOPT THE YUMA COUNTY SECURITY STANDARDS POLICY:

Adopted this 17th day of July 2017



MARCO A. "TONY" REYES, Chairman

ATTEST:



SUSAN K. THORPE
County Administrator/Clerk of the Board

APPROVED AS TO FORM AND DETERMINED TO BE WITHIN THE SCOPE OF PERFORMANCE OF DUTY OF THE YUMA COUNTY BOARD OF SUPERVISORS:



JON R. SMITH, County Attorney

1. Purpose

This policy establishes the minimum information security standards, for managing risks from inadequate information security through the establishment of an effective security program. This will assist Yuma County to implement security best practices with regard to enterprise security planning, preparation, and strategy.

2. Scope

This policy applies to all Information Technology Resources (ITRs) owned or operated by Yuma County as a government entity. All Users of said IT resources are responsible for adhering to this policy. Any information or systems not specifically identified as the property of other parties which is used to transmit, modify, store or view data (including e-mail and system files) is the property of Yuma County. To be in effect, this policy and any future proposed amendments must be submitted to the Yuma County IT Steering Committee for review and adopted by the Yuma County Board of Supervisors. All amendments will be addressed in accordance with Paragraph 5, below.

3. Intent

It is the intention of this policy to establish minimum security standards throughout Yuma County and its business units to help ensure the confidentiality, integrity, security, and availability of ITRs so to be consistent with best practices associated with organizational information security management.

4. Office of Primary Responsibility

The Yuma County Chief Information Officer (CIO) assisted by the IT Security Division (ISD) is responsible for the development, coordination, maintenance, and distribution of the Yuma County Information Security Standards Policy. The ISD shall aid in the development of any necessary process charts and procedures which support the implementation of this policy for sub-agencies/organizations requiring assistance. See the Supplemental Document area for a visual overview for policy applicability.

5. Change Control Procedures

All recommendations for amendments to the policy shall be discussed and reviewed by the Yuma County IT Steering Committee (ITSC) for final action based on recommendations by the CIO. If approved, the recommendations will be included as an Agenda item for the next available regularly scheduled Board of Supervisors meeting for discussion and possible action. If the changes are adopted by the Board of Supervisors, the Policy shall be updated with the revision number, and effective dates changed for Policy redistribution. Copies of the current Policy shall be made available upon request.

6. Policy Exceptions

All requests for exceptions must be reviewed and approved by the CIO and the ISD. Requests for exceptions will be reviewed for validity and are not automatically approved. Requests for exceptions that create a significant risk to the County without compensating controls will not be approved. Requests for exception will be reviewed quarterly to ensure that assumptions or business conditions have not changed. Renewals are not automatically approved.

If a particular exception is granted, future requests of the same type will receive the same approval, barring special circumstances. If a certain type of exception is constantly being requested or approved, it may mean that relevant policies or standards need to be adjusted to include the exception as a norm. The ISD will review these patterns and recommend changes as needed.

Requests for exceptions will be revoked in the event of a security incident or policy violation using established incident response procedures.

7. Policy Statement

The ISD shall act as the centralized office for determining County IT security policies and implementation strategies including identifying security requirements, determining the computer systems affected, determining the security controls/methods to be implemented, implementing/administering the necessary controls, monitoring security status, and conducting security audits.

The controls specified in this policy are mandatory minimum standards that are applicable to all Yuma County owned and operated ITRs to include both local or wide-area networked resources that process, store, or transmit information, wherein:

- There is a risk that County Information Technology Resources or information could be misappropriated;
- There is a risk that privacy legislation could be violated;
- The loss of such a system or information could impair the ongoing operations of the County; or
- Criminal Justice Information System data could be viewed by unauthorized personnel.

The degree of internal control shall be based on an assessment of the County's potential exposure to theft, destruction, alteration, or misuse of ITRs. These control techniques shall be considered in the implementation, and use of all County owned and operated ITRs, including, but not limited to:

- County owned computers and workstations;
- Public-facing applications/websites;
- Data Servers;
- County owned/licensed software;
- Voice communication systems;
- Switches/Routers/Firewalls;
- Backup power services (Uninterruptible Power Supplies, etc.);
- Data network communications;
- Virtual Private Networks (VPN);
- County owned mobile devices (Both voice and data);
- Local Area Networks (LANs);
- Wireless Local Area Network (WLANS);
- Wide Area Networks (WANs);
- Wireless Wide Area Networks (WWANs); or
- Antennas and other rooftop connectivity hardware;

Primary access controls shall be implemented using both hardware and software system security options on Host Computers, network servers, Stand-Alone Systems, and communications devices. These options may be supplemented with add-on packages and manual procedures, as necessary, to meet protection and auditability requirements.

8. Risk Assessment

Security and controls shall be applied in a manner that is consistent with the confidentiality and value of the information to the County. In determining the level of security control, ITD System Administrators or ITD managers shall conduct risk assessments to computing and information resources in a manner consistent with this policy and balance the costs of protecting the resources against the potential exposures where the threat is the source of a potential security breach and risk is the likelihood of a breach occurring. Appropriate security measures will have been attained when the cost of protecting ITRs and data against identified risk is balanced with the cost of exposure.

9. Accountability

The ISD shall work with System Administrators, Network Managers, Security Administrators, and Agency Heads to ensure that adequate controls are established, documented, and observed for all County ITRs. The controls and documentation shall be reviewed annually to determine the adequacy of controls and compliance with this Policy.

The ISD shall assist with the development and/or provide technical assistance and guidance to each IT Department (ITD) in their development of written security standards, policies, and procedures. The existence of security policies and procedures in no way absolves any system users working in support of the County from their individual responsibility to protect the integrity of the County ITRs and data.

10. Security Administration

The IT Security Administrator is the designated body for all of IT security operations within the County and is delegated the responsibility of developing policies, procedures, and standards regarding the transmission, processing, maintenance, safeguarding, and disposal of information; developing training and informational materials; and assessing and ensuring the County's compliance with applicable laws, regulations, policies, procedures, and standards relating to information retention, security and privacy.

All incidents involving County owned ITRs must be reported to the IT Security Administrator.

Each ITD that has primary use of a Host Computer and/or Local Area Network (LAN) system shall designate a local IT Security Custodian (ISC) who will be responsible for all system security, including user registration and monitoring of security-related events. In most cases, the ISC may be the same person who has network/system administrator responsibilities for the system. The ISC shall consult with the ISD on all security related matters to ensure compliance with this Policy.

The ISD shall perform this function for any system at the request of ITD managers.

Wide Area Network (WAN) security and system administration shall be performed by designated network personnel and ISCs. Close coordination between all County Agencies and Organizations that have primary use of a Local Area Network shall be maintained to ensure remote access is controlled within acceptable parameters established by the Agency or Organization.

11. Operating Systems

Any software updates or patches related to the security of ITRs shall be installed as soon as they are received from the system software vendor, provided that sufficient testing has occurred and if deemed beneficial.

12. Physical Security

The ISD shall aid in and conduct quarterly inspections of physical precautions in place for all ITRs and notify Department/Agency/Organization heads of security problems and corrective action recommendations. Physical access to computing resources must be controlled and environmental precautions provided to limit the possibility of accidental or intentional damage from natural or man-made causes.

- Critical system components, including servers, switches, routers, firewalls, SAN's, network control centers, and system consoles shall be secured using theft- deterrent and/or physical security devices.
- Anyone requiring access to rooms that house ACJIS systems is required to poses a "D" level certification or must be accompanied by a certified and authorized escort.
- Surge suppressors or voltage regulators shall be used on all critical or high-value components to protect against power fluctuations.
- Each ITD shall maintain a complete equipment inventory in accordance with the County Computer Inventory Control Policy.
- Distribution and use of all diagnostic hardware and software shall be closely controlled and monitored. Particularly communications and network diagnostic equipment such as protocol analyzers and sniffers.
- All wiring and communications cabinets shall be physically secured. Cabling and wiring shall not be exposed or unprotected and shall be inspected quarterly by their respective ITDs.
- Uninterruptible Power Supplies (UPS) shall be used on all critical systems to protect against loss of critical services and information in the event of power outages. Consideration should be given to the value of any software-controlled shutdown capabilities that the UPS my offer in the event that power outages exceed the battery backup runtimes.

13. Information Security

- A. User Identification and Authentication: Host Computer and network system access controls are required to ensure that only authorized persons are using the system resources and information necessary to perform their job duties. Access shall be controlled by use of log-on identification, which identifies the user to the system, and a password, which verifies the user.
1. All users shall be assigned unique log-on identification by the System Administrator. Each user shall enter an obscure password when logging on for the first time. All passwords must be at least eight (8) characters long. Passwords must contain at least one letter, 1 number, and one special character such as #,@,! etc.
 2. The ITD System Administrator shall require the Host Computer or networked ITRs to prompt users to change their personal password on a recurring basis. Thirty (30) days is the maximum acceptable duration between mandatory password changes. Passwords must not be the same as any of the previous six (6) passwords. User passwords shall not be echoed (readable on the monitor or terminal screen) during log-in. Passwords to systems not tied to Active Directory or similar enterprise management systems should be changed at the same time for purposes of consistency.
 3. Administrator user names and passwords to Host Computer or networked ITRs shall be protected via an encrypted file.
 4. If a password needs to be reset, the System Administrator will set a password that expires after the first login and will not know the user's new password.
 5. After a specified number of unsuccessful log-on attempts (No more than four (4) within a 15-minute period), the system shall automatically disable the log-on identifier until reset by the System Administrator or until a specified amount of time has passed.
 6. The Human Resources Department must notify the appropriate ITD immediately when an employee has separated from the County in order to protect County systems from unauthorized access. All accounts associated with the separated employee shall be suspended at this time.
 7. Log-on identifications shall be suspended after 60 days of non-use and eliminated after 120 days of non-use.
 8. ITD System Administrators for Host Computers and networks shall be responsible for educating users on log-on procedures and proper methods of using secure passwords. It is required that:
 - Users not log-in to more than one device at a time unless specifically authorized to do so.
 - Users logging on to a device at other than their usual workstation, log off as soon as the task is finished.

- Users lock their workstation when leaving the area.
 - Workstations automatically protect after 15 minutes of inactivity.
9. If the Host Computer or networked ITR has the capability to display date/time of the last logon, this feature shall be utilized so that each user can verify that his or her identification has not been used by anyone else.
 10. User workstations must not run any server software such as FTP, TFTP, Web Services, or any remote control server such as PCAnywhere, LAPLink, TeamViewer, Join.me, VNC or LogMeIn. Workstations must be configured to prevent unauthorized installation of software by users. Any remotely administered systems must be signed off by their respective ITDs and reported to the ISD and County CIO to ensure compliance with County, State and Industry policies and regulations.

B. Host and File Server Controls:

1. All Host Computer operating system installations and subsequent changes shall be performed by the ITD or authorized contractor/vendor. File server network operating system installations and subsequent changes shall be performed by the ITD or authorized contractor/vendor. Any changes (whether performed by contractors/vendors or IT Staff) to host computer or network operating systems shall be coordinated with the primary users of the system and documented using established change control procedures created by the overseeing ITD.
2. Host Computers and File Servers shall not be left unattended when operational unless they are located in a secured area.
3. ITD System Administrators shall ensure that all operating system software and applications software loaded on Host Computers or File Servers are in compliance with licensing requirements/agreements. Each ITD is responsible for ensuring that operating system software and application software loaded on individual computers and IT assets (including Phones, Tablets, and Mobile Computing Devices) is in compliance with licensing requirements/agreements.
4. ITD System Administrators shall ensure that all network drives are backed up before loading any new software and scanned for viruses periodically, especially after the installation of new software. Individual computers (including laptop or notebook computers) shall also be backed-up before loading any new software and scanned for viruses periodically, especially after the installation of new software.

C. Audit trails, Security Violation Reports, and Notifications:

1. Host Computers and File Servers shall include logs and audit trails to detect and report unauthorized access attempts.
2. Audit trails shall include the source/location of unauthorized attempts, log-on identification, date/time of the event, and target or requested services.

3. Audit log files shall be accessed only by the ITD System Administrators and ISCs.
 4. Audit log file information shall be reviewed by the ITD System Administrator or ISC at least weekly.
 5. For compliance purposes, there should be a minimum retention period for security records. Retention periods may be dictated by specific industry and compliance standards. At a minimum, the general retention schedules identified by the Arizona State Library, Archives and Public Records Division must be followed. All IT security violations and incidents must be reported to the ISD for documentation.
 6. Each ITD is responsible for the security and protection of Computer and Information Systems used by their respective users. The ISD, in accordance with Sections 7 and 13 of this policy, shall on a quarterly basis conduct physical and procedural security audits of Computer and Information Systems to ensure the confidentiality, integrity, security, and availability of the systems remain uncompromised. Audits performed by the ISD shall be documented, and a report of adverse findings shall be provided to the Agency Head.
 7. Corrective actions plans for adverse findings involving employees shall be developed by the Agency Head with consultation from Human Resources prior to any discussion with the employee and tracked until all adverse findings have been resolved.
- D. Software Integrity/Anti-Virus Software:
1. System Administrators/ISCs shall ensure that all copied software (particularly shareware) is verified to be free of computer viruses, worms, and Trojan Horses before loading it onto the Host Computer or File Server. Licensed software received directly from software vendors in sealed packages shall be exempt from this requirement unless the Administrator is unsure of the reliability of the software vendor.
 2. System Administrators/ ISCs shall ensure that anti-virus software is resident on all computers and IT assets connected to Host Computers or File Servers.
 3. All devices containing Sensitive Information shall be encrypted. This is applicable to all County owned ITRs used outside of County data and communication networks.

14. Host and File Server Network Security

A. Communications Controls:

1. All Host Computer and File Server network configuration changes shall be processed through change control procedures established by the overseeing ITD.
2. All Host Computer and File Server data communications connections and configurations shall be accomplished or coordinated through identified ITDs whether performed by County resources or contractors/vendors.
3. All data communications ports shall be made unavailable for any new session until the prior session has been properly disconnected.

4. Data communication intruder detection capabilities shall be made available and utilized.
 5. The Host Computer and File Server System Administrator/ISC shall ensure that users can connect only to those resources for which they are authorized.
 6. All access to Host Computer and File Server networks shall be traceable to the login identification.
 7. All Host Computer and File Server network connections shall be reviewed monthly to ensure that protection has not been degraded.
- B. System Status/Warning Banners:
1. No system information shall be provided before the user logging-on has supplied a valid password.
 2. Log-in banners should appear on all systems alerting user's to acceptable system use and or monitoring. Log-in banners shall not contain a general welcoming message.
 3. IT assets, when possible, shall have an automatic screen lock enabled. A user password shall be required to log back in. Exempt systems include kiosks, reference computers or systems used by the general public.
- C. Remote Access Controls:
1. ITD System Administrators/ ISCs shall have the capability to control on-site and off-site remote access to Host Computers, File Servers, and Stand-Alone Computers.
 2. ITD System Administrators/ ISCs shall control and document users that are authorized to have remote access to any County ITR, particularly if the IT resource is also connected to a File Server or Host Computer network.
 3. Remote access information such as telephone numbers, IP addresses, authorization codes, log-on identification, passwords, digital certificates and dialing/log-on procedures shall be protected from unauthorized disclosure.
 4. All County remote access hardware, such as VPN devices, shall be physically secured from unauthorized access or use.
 5. Modems shall be prohibited on individual computer workstations that are connected to a network or Host Computer.
 6. Mobile computers shall be configured as to disable the modem when the network card is enabled and vice-versa.

15. Continuing IT Security Program

As the office of primary responsibility for ensuring the security of County information, the CIO via the ISD endorses a continuing IT Security Program. The purpose of the program is to address emerging security issues arising from technological advancement while maintaining security and privacy. LANS, integration of County-wide computer networks, interconnectivity to non-County networks, and e-mail systems necessitate careful planning to ensure productivity benefits are balanced against security requirements. The County Information Security Standards Policy and the continuing IT Security Program are predicated on the following basic assumptions:

- A. Information stored and processed on distributed processors and transmitted across networks should be as secure as any other Stand-Alone or closed computing platform;
- B. Networked resource performance and function should be balanced with the appropriate levels of security and controls;
- C. Security controls should prevent unauthorized users from accessing or modifying information on networked resources; and
- D. Computer information security policies should have equal acceptance and implementation priority as all other policies and implementation plans.

16. Definitions

- Agency Head - The head of any County department or agency and any other officer or employee of any department or agency to whom authority has been delegated.
- Arizona Criminal Justice Information System (ACJIS) – The central state repository created in order to collect, store and disseminate complete and accurate Arizona criminal history records and related criminal justice information. The ACJIS network is maintained by the Arizona Department of Public Safety and is available to authorized local, state, and federal criminal justice agencies in accordance with A.R.S. § 41-1750.
- Availability- The ability to access specific electronic information within a specific time frame, and the degree to which a system or component is operational and accessible when required for use.
- File Server – A computer used mainly or exclusively for storing and supplying data files generated and/or required by other computers in a network.
- File Transfer Protocol (FTP) - a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections
- Host Computer(s) - A centralized or main computer system that provides data and computing services to other systems via a network.

- Information System(s) - Any mechanism used for acquiring, filing, storing, and retrieving an organized body of knowledge. Information systems include hardware, software, firmware, procedures for use of the system by people, services intended to provide support to the operation of the system, any equipment or interconnected system or subsystems used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.
- Information Technology Resource (ITR) – Any electronic, computing, and communication asset owned and or operated by Yuma County.
- Information Technology Steering Committee (ITSC) – A collaboration and consensus-driven IT governance committee which aligns, prioritizes, and sustains the County's IT strategies and objectives.
- IT Department (ITD) – The department that is charged with establishing, monitoring and maintaining information technology systems and services. (Yuma County ITS, Sheriff's Office IT Support, and Library IT Services)
- IT Security Custodian (ISC) - A person who has technical control over an information technology asset in relation IT Security operations.
- Network Manager - A person who manages a local area communications network (LAN) or wide area network (WAN) for an organization.
- Privacy Legislation- Any law governing privacy such as the United States Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act.
- Security Administrator - The primary individual responsible for managing, monitoring, and administering security over one or more computer networks. Security Administrators typically design and implement network security policies across the network.
- Security Record – Any records relating to the security of systems and data. This is not limited to audits trails, incident handling records, legal and regulatory compliance records.
- Sensitive Information – Any data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.
- Stand-Alone Computer/System - A desktop, laptop computer or device that is used on its own without requiring a connection to a local area network (LAN) or wide area network (WAN).
- Storage Area Network (SAN) - A specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

- System Administrator – A person who is responsible for the design, deployment, upkeep, reliability, and security of computer networks or systems, especially in a multiuser environment. They manage the computing needs of all users within an organization.
- Trivial File Transfer Protocol (TFTP) - An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP).
- User – Any person who uses or operates a County owned computer, network or electronic device.
- Virtual Network Computing (VNC) – An unsecured graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network
- Virtual Private Network (VPN) - A technology that creates a safe and encrypted connection over a less secure network, such as the internet.

17. Supplemental Documents

