

Maricopa County Policies and Procedures	Subject: Electronic Information Resource Security	Number: A1605 Issue Date: 2/95
Approved: David R. Smith	Initiating Department: Technology Management and Policy	

A. Purpose

". . . public records are the people's records, and . . . the officials in whose custody they happen to be are merely trustees for the people."

As "trustee" of the people's records, Maricopa County government is responsible for maintaining and preserving the information entrusted to it, assuring prompt access to information, and for securing the confidentiality of information that is not subject to disclosure in the best interests of the proper functioning of the county.

The advent of computers (and related technology) has afforded government tremendous new powers to manage and distribute information. However, these powers have not come without attendant dangers, problems and limitations. The intent of this policy is to assure that Maricopa County government's implementation of its electronic information resources will continue to maintain the people's trust by establishing a framework to address the access and security requirements associated with information derived and transmitted from its information management systems.

B. Policy

Information is a county asset and must be appropriately evaluated and protected against unauthorized use, disclosure, theft, modification, destruction, or denial of access. The protection and security of information resources is the responsibility of each elected official, appointed department director, and all employees.

Each elected official and appointed department director shall establish security controls and practices sufficient to ensure that confidentiality (to the extent required by law), integrity, availability, and appropriate use of all electronic data and information assets will be maintained for information systems.

The Board of Supervisors has established a standing Electronic Information Resource committee, chaired by the Chief Information Officer.

Elected officials and appointed department directors shall create and adopt a departmental security policy (including provisions for appropriate use) for information, information systems, and for the transmission of information which shall be approved by the Electronic Information Resource Committee.

All contracts and agreements with contractors of Maricopa County agencies, and other personnel or organizations that process information using a computer system on behalf of Maricopa County shall require compliance with the Maricopa County Security Standards Manual.

Maricopa County departments acquiring Information Technology will ensure that procurements comply with the Maricopa County Security Standards Manual.

C. Definitions

An "Electronic Information Resource" is data and information generated, stored, and/or transmitted by information systems.

An "information system" is any mechanism used for acquiring, filing, storing, and retrieving an organized body of knowledge. Information systems include hardware, software, firmware, and 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.

The "Maricopa County Security Standards Manual" is a document published by the Electronic Information Resources committee that establishes and describes county-wide minimum technical, physical, and personnel safeguards, including procedures and practices.

"Logical Security" is an intangible process that identifies, authenticates, authorizes and provides access control over programs and data. A password is an example of logical security for data stored or transmitted.

"Physical Security" refers to material factors (facility, environment, communication wiring, devices). Anchoring PC's with locks is an example of a physical security item.

"Integrity" is the quality (accuracy, precision, consistency, reliability) and time dependent state (current, historic, archive) of data required by the business to meet its present and future goals.

"Availability" is 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.

D. Authority and Responsibility

The Office of Technology Management and Policy shall:

chair the Electronic Information Resource committee.

be accountable to the County Administrative Officer for overseeing the County's electronic information resource security program.

The Electronic Information Resource committee shall:

be comprised of a chairperson, one member representing the interest of the County Attorney's Office, one member representing the interest of the Department of County Counsel, one member representing the interest of the Human Resources Department, one member representing the interest of the County Auditor's Office, and three members from the Office of Technology Management and Policy representing the interest of the technology community.

publish and maintain the Maricopa County Security Standards manual. This manual will provide the minimum standards for elected officials, and appointed department directors to establish policies and procedures in compliance with county-wide electronic information resource security. The manual establishes minimum standards covering all aspects of security including: physical and logical security; security administration; security assurance; risk assessment; telecommuting; data classification; and, the processing, distribution, transmission, storage and backup (current and archive) of electronic information resources.

reviews and approves departmental security policies adopted by elected officials and appointed department directors.

shall appoint subcommittees comprised of representatives of technical and non-technical community as needed to establish more detailed specifications and standards relating to technical compliance.

Elected officials and appointed department directors shall:

adopt a department specific security policy and submit to the Electronic Information Resource committee.

establish security controls sufficient to ensure the confidentiality, integrity, availability, and use of electronic information resources for which they have responsibility. Departmental standards, procedures and practices developed for the protection of County electronic information resources must be consistent with the Maricopa County Security Standards Manual.

establish a security officer function within their department. The protection of electronic information resources and information systems are part of that individual's responsibilities.

conduct security awareness programs for all their employees.

perform periodic assessments of the vulnerability of their electronic information resources and information systems to internal and external threats that may cause destruction, modification, denial of access, and/or unwarranted disclosure.

Departmental Security Officers shall:

be responsible for investigating reports of exposure, misuse, loss, theft of county information, or its falsification or alteration. Summary security audit compliance reports will be forwarded to the Electronic Information Resource committee.

County Employees shall:

be responsible for understanding and complying with county-wide and departmental standards, practices and procedures regarding the protection of county electronic information resources and information systems.

The County Auditor shall:

within the scope of information systems audits include compliance with county-wide and departmental security standards, practices and procedures.