

ADMINISTRATIVE PROCEDURES



Procedure Number: 27-10

Effective Date: 10/1/2009

Revision Date: _____

C. Duluth
County Administrator

SUBJECT: COUNTY ADMINISTRATOR IT ENVIRONMENT ACCESS CONTROL

DEPARTMENT RESPONSIBLE: ALL COUNTY DEPARTMENTS

I. PURPOSE

This administrative procedure establishes base line Information Technology (IT) Access and Control practices which must be implemented and maintained by IT organizations within Pima County.

II. DEFINITIONS

IT resource: The County's network and infrastructure components through which all County personnel control facilities, access business applications as well as access, create, store and print documents

Business applications: Computer software that has been internally developed or purchased/configured to automate and/or control (e.g. SCADA) Specific County, departmental or division business processes.

IT environment: The County's information technology resources, and business applications utilized by County personnel to perform their job responsibilities and duties. This IT environment includes, but is not limited to, business applications, telephones, cell phones, personal digital assistants, pagers, radios, electronic mail (includes voice), computers, connectivity technologies used to access these communication devices, Internet access, as well as fax, printer, scanner, and copier machines.

Sensitive and Confidential Information: Any information which is governed by federal, state or local legislation restricting access for public use and consumption (e.g., HIPAA). This also includes information under development to be released to the public at a future date, or information that could cause harm to the County and its Constituency (e.g., computer passwords or inappropriate access to critical control systems).

III. PROCEDURE

Physical Access - The County maintains physical computing center facilities which provide IT resources and business applications utilized by County personnel to perform daily job responsibilities and duties. Each of these centers must:

- A. Utilize a documented Physical Access Control procedure which ensures that physical access is limited to appropriate individuals with a direct need for access;
- B. Require approved physical access request and approval documentation from the authority accountable for the security and operation of the center;
- C. Use a process which adds changes or removes access for individuals as their job responsibilities change over time.

Logical Access – The County provides access to business applications and IT resources utilized by County personnel to perform daily job responsibilities and duties. Each IT organization which controls an individual's access to this IT environment must:

- A. Utilize a documented Logical Control Access procedure which ensures that access is consistent with the individual's job responsibilities and duties;
- B. Require approved logical access request and approval documentation from:
 1. the individual's department management,
 2. the owner of a business application or the owner's delegate, and/or
 3. information technology resource owner.
- C. Use a process which adds, changes, or removes access for individuals as their job responsibilities change over time.
- D. Limit the use of generic access accounts to those that are read only.
- E. Ensure periodic review of audit trails which allow monitoring of activity within applications that have financial, public safety or compliance impact.

Password Security – Each IT organization within the County which provides and/or controls access to IT resources and business applications must ensure that strong passwords are utilized within the IT environment. Pima County's strong password rules are defined in the Information Technology Department guideline ITG 8-01-2009. Each IT organization must also use a documented procedure for managing the password environment within their span-of-control (which includes specialized accounts specific to their IT organization).

(Legacy systems that are incapable of adhering to the above practices are exempt from this strong password requirement. Any new business application or IT resource implemented in production from calendar year 2010 forward must adhere to the above strong password requirement).

Change Management – Ensuring proper management approval of changes to an IT environment helps safeguard financial, sensitive and confidential information from misstatement, fraud, loss or unintended or unauthorized changes. Each IT organization within the County therefore must:

- A. Implement a comprehensive change management procedure, whose purpose is to ensure that all changes to the IT environment are appropriate, authorized and adequately tested and reviewed.
- B. Implement standardized change management request forms that include an appropriate level of detail and authorization.
- C. Develop and maintain a comprehensive list of individuals who are authorized to approve any IT environment changes and ensure the changes are not made without appropriate documentation and approval.
- D. Ensure that the change management forms are appropriately tracked and maintained.
- E. Periodically monitor system-generated audit logs and reports that track IT environment changes.