PINAL COUNTY POLICY AND PROCEDURE **2.45**

Subject: Use of Login Banners to provide legal Notice to Users

Date: **October 22, 2008**

Pages: **1 of 3**

Replaces Policy Dated: N/A

PURPOSE: As a requirement for successfully prosecuting those unauthorized users who improperly use a Pinal County computer.

APPLICATION: This policy applies to all Pinal County IT employees, other county employees, temporary employees that utilize Pinal County computers.

DEFINITIONS:

IT POLICY:

Pinal County computers will have a warning banner displayed at all network access points. This policy will comply with the U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division. Reference: CJIS Security Policy June 2007 Version 4.4
The banner must warn authorized and unauthorized users:

- About what is considered the proper use of the computer system.
- The system is being monitored to detect improper use and other illicit activity.
- There is no expectation of privacy while using this system.

AUTHORITY AND RESPONSIBILITY:

1. IT Employees are responsible for:

    a. Understanding and adhering to IT policy protocols.
    b. Using common sense and good judgment as determined by this IT Policy and the Chief Information Officer.

2. IT Management is responsible for:

    a. Understanding IT policy protocols and related policies.
    b. Advising their staff about this policy and appropriate use.
    c. Monitor and Audit use of this policy.
    d. Notifying CIO of non-compliance issues related to this policy.
    e. Applying progressive discipline procedures for non-compliance of IT staff in relation to this IT policy. (Reference: Pinal County Rule 12)

FORMS:

1. Information Technology Department Acknowledgement Forms

==========

ADDENDUM A

PROBLEM: Failure to have notification might be used as a defense in the prosecution of a user or intruder for improper use of the system.

SOLUTION: Make the modifications described here to add banners to all access points on your system. Where it is not possible to implement automatic electronic banners, a printed banner should be attached where it can be read by the user of the system.

Creating/Installing Warning Banners

1. Pinal County Government is requiring warning banners on all interactive access points (for example, console login, telnet, ftp, and http) and on all non-interactive access points that provide a human readable response (for example, finger).

2. The County prefers that banners are displayed prior to access to system resources and that the user must acknowledge that compliance before the user can access those resources. In the event that the system does not support this pre-login capability, the system should display a warning at or immediately after login.

3. In the event that electronic banners and warnings are not supported by a system, printed banners should be used that are clearly visible to the user as they use the system.

NOTE: This document will change as the IT department identifies and determines new entry points and access methods.

The Board of Supervisors and the IT department has approved the following banner for county computer systems.

****

NOTICE TO USERS

Warning! The use of this system is restricted to authorized users. All information and communications on this system are subject to review, monitoring and recording at any time, without notice or permission. Users should have no expectation of privacy. Unauthorized access or use shall be subject to prosecution.

****

Warning Banner Modification for Public Servers

==========

Public servers such as public web servers and anonymous ftp servers that are available to the general public must also have a banner. Public servers are those that allow access by anyone who can connect to the server over a network through a normal access point without requiring any authentication. The banner must indicate to the user that they have no expectation of privacy while using the server and that all access to the server is logged. The banner below is an example of such a public banner for a public web server. This public banner is only for the public access points to a server. Nonpublic access points to a server must still display the warning banner above.

****

NOTICE TO USERS

Use of this system constitutes consent to security monitoring and testing. All activity is logged with your host name and IP address.

****

The technical details for implementing banners is dependent on the particular operating system and access point refer to Procedures for Creating Login Banners.