Peoria Police Department
Policy and Procedure Manual

Policy 8.06	Computer System Security

I. POLICY

It is the policy of this Department to ensure that all computerized systems accessed by agency employees are maintained and managed in a protected and secure environment.

II. PROCEDURE

A. Administration: System Security Officer (SSO): The Technical Services Bureau Manager has been designated by the Chief of Police as the System Security Officer (SSO) for the Peoria Police Department. The primary duties of the SSO are as follows.

1. Acts as liaison between the Peoria Police Department and Control Terminal Agency (Arizona Department of Public Safety (AZ DPS)). All requests concerning the Arizona Criminal Justice Information System (ACJIS), the National Crime Information Center (NCIC), and the Combined Agency Research Network for the Analysis of Crime (CARNAC) must be coordinated through the Department's SSO.

2. Ensures that Department personnel are in compliance with all applicable laws, rules, regulations, policies, and procedures governing the ACJIS network and the Computer Aided Dispatch (CAD)/Crimes computer programs, as well as all computer software installed in City owned computers within the Peoria Police Department.

3. Manages record validations, quality control, ACJIS system security matters, operations audits, and/or any problem concerning the ACJIS and the CAD/Crimes programs.

4. The Department's SSO is responsible for ensuring that all record transactions in the ACJIS/NCIC system are timely and accurate by performing monthly validations of selected entries.

B. Arizona Criminal Justice Information System (ACJIS) (82.1.9)

1. Access Rights: The SSO, in coordination with the applicable Bureau Manager/Lieutenant, will determine access authority to the ACJIS system. Access rights are granted on a need-to-know basis to law enforcement employees only.

   a. Once authorization rights have been established, it requires the combined efforts of the City of Peoria's Information Technology (IT) Department, the AZ DPS, and the SSO to perform set-up requirements of both the workstations and end users prior to employees being capable of accessing the system.

   b. Employees accessing or entering ACJIS record information are required to obtain a Terminal Operator (TOC) Certificate within six (6) months of using the system. The Technical Services Bureau oversees TOC testing on a regular basis for all new employees as well those employees needing to renew their certificates.

2. Authorized Access: The following job positions and applicable workstation computer devices have been authorized to access the ACJIS system:

   a. Chief of Police

   b. Deputy Chief

   c. Commanders

   d. Patrol Lieutenants

   e. Technical Services Bureau Manager (SSO)

f. Sergeants

g. Patrol Officers (Report Writing Room, MDCs)

h. Detectives (Criminal Investigations)

i. Crime Analyst

j. Administrative Assistant (Criminal Investigations only)

k. Communications Supervisors

l. Communications Specialists

m. Records Supervisor

n. Records Employees

o. Police Services Officers (Property and Evidence)

p. Station Officers

3. Law Enforcement Inquiries Only: Use of the ACJIS and CARNAC systems are restricted to law enforcement inquiry purposes only. Inquiring into the systems for personal reasons is a violation of both State and Federal law. Additionally, secondary dissemination of information obtained from either of these systems is prohibited.

   a. All inquiries/entries made into the ACJIS or CARNAC systems are logged automatically at AZ DPS. In cases in which an allegation has been made of system misuse, the SSO may obtain a log search from AZ DPS to determine:

      (1) If the misuse actually occurred, and;

      (2) If the misuse did occur, from which computer or Mobile Data Computer (MDC) the inquiry(s) was initiated from. Upon determining the device identification, the user signed-on to that computer/MDC at the time of the inquiry can then be determined.

   b. Employees accessing ACJIS data from either a desktop or MDC device are prohibited from copying/cutting and pasting the data to a secondary application source (ie, CAD, MicroSoft (MS) Word, Outlook, etc).

C. Departmental Systems (CAD/Crimes)

1. Access to the Department's CAD/Crimes system is determined by work groups. The work group identification for access rights into the CAD/Crimes system can be obtained by contacting the Peoria Police Department's System Security Officer.

2. AS400 Password:

   a. All CAD/Crimes modules require the use of the employee's AS400 password before accessing the various components.

   b. Employees attempting to sign the AS400 without a valid password will be disabled after three (3) attempts.

      (1) Invalid attempts into the AS400 are reviewed for possible system misuse on a regular basis. (82.1.6)

      (2) Suspected system misuse violations will be immediately reported to the Chief of Police in writing.

3. CAD/Crimes modules in which an employee has not been granted access rights will not be displayed as menu options on their computers.

4. Security History File: Access into all CAD/Crimes modules is automatically logged into the Security History file. The Security History log file contains the following information.

    a. Access Type

    b. Incident Report number, if applicable

    c. Time of access

    d. Program Name

    e. User ID

    f. Workstation ID

5. The Security History file is purged every two (2) years.

D. AS400: The AS400 is the mainframe in which the CAD/Crimes programs reside. Prior to accessing any of the modules located in these programs, the employee must have AS400 authority.

1. User ID's and passwords for the AS400 are established by the City of Peoria's IT Department.

    a. The Administrative Secretary notifies the IT Department of all newly hired personnel at which time a User ID and Password are established.

    b. The Technical Services Bureau Manager, Records Supervisor, and Communications Supervisors may reset expired or disabled passwords for existing employees.

    c. AS400 user passwords are set to expire automatically every thirty days. Employees will receive a seven (7) day advance notice informing them that they must change their password.

    d. Neither the SSO nor IT system security personnel can view AS400 user passwords. In the event that an employee does not recall his or her password, a new password will need to be established.

2. To ensure system integrity and to protect the individual employee, the sharing of passwords is strictly prohibited.

3. Employees attempting to access the AS400 using an invalid password will cause the User ID to be disabled after three (3) attempts.

    a. The SSO monitors invalid password access attempts on a regular basis using the AS400 History Log. (82.1.6)

    b. All unexplained or questionable access attempts will be immediately reported, in writing, to the Chief of Police.

4. On an annual basis, the Technical Services Bureau Manager will review all Peoria Police Department AS400 User ID's to ensure that personnel no longer authorized to access the AS400 system have been placed in a disabled status. (82.1.6)

E. iSeries/AS400 Back-ups

1. The iSeries/AS400, which houses both the CAD/Crimes software programs, is backed-up as follows by IT personnel. (82.1.8):

    a. Daily - Five days a week (Monday through Friday) data is backed-up. Data is retained for a minimum of one (1) month before the media is available for reuse.

    b. Monthly - A copy of the last Friday of the month data is retained for a period of one (1) year before reuse.

    c. Annual - A complete backup of all data is accomplished on an annual basis.

2. All back-up tapes are retained in a secure off-site facility and are transported by off-site personnel in a locked metal case.

F. User Access upon Employee Separation: Immediately upon receipt of any Personnel Orders advising of employee separation, the Technical Services Bureau Manager will delete the user from AS400 access and notify the IT Department to disable the employee's access to both the City of Peoria network and telephone system.

Peoria Police Department
Policy 8.06 Computer System Security
Original Issue Date: 01/01/03
Last Revision Date: 01/18/07
Next Review Date: 11/30/07
Office of Primary Responsibility: SSD
Editor: M. Mugavero
Reviewed By: S. Lekan

APPROVED: _____
Larry J. Ratcliff
Acting Chief of Police