7100 CRIMINAL INFORMATION SYSTEMS (Revised December 30, 2014)

7110 ARIZONA CRIMINAL JUSTICE INFORMATION SYSTEM (ACJIS)

7111 Administration

The CJIS system is a series of databases maintained by the Department of Public Safety (DPS) to be used by the law enforcement and criminal justice practitioners.

7112 Testing and Certification

Terminal Operator Certification (TOC) is a process required by DPS in conjunction with the United States Department of Justice. All law enforcement personnel with access (through assigned laptops, personal computer, etc.) to the various state and federal databases that make up CJIS are required to demonstrate an understanding of the information available to them and the laws and policies governing release of that information. A passing grade on a test created by the DPS Audit Unit is required to acquire certification. Re-certification is required biennially. The Records Superintendent administers both activities.

7113 Security of Information

Any employee who has a Terminal Operator Certificate (TOC) may access Criminal Justice Information System (CJIS) data provided it is for law enforcement purposes. Additionally, employees who are not certified for CJIS access may request and receive CJIS data from employees who are certified provided it also is for law enforcement purposes. Employees who are not certified for CJIS shall not access CJIS.

7120 ACCESS TO ACJIS DATA

7121 Dissemination of Arizona Criminal Justice Information System (ACJIS) Data

The Records Superintendent or designee(s) shall be the only personnel who can release information obtained through the ACJIS computer network to the public or other law enforcement agencies. (An exception: when officers from other agencies have a mutual interest in a specific case that TPD is working, those officers can receive ACJIS information that is obtained from TPD terminals). This release shall be based on the requirements set forth in federal and state laws, NCIC/ACIC rules and regulations, AJCIS rules and TPD *General Orders*.

7122 ALERT Files

7122.1 Entry Requirements

Information relative to individuals perceived as a potential danger to police officers may be entered into the Records Management System (I/Leads) with a Name Flag Alert file. Officers wishing to enter a name shall select the appropriate tab in the record program and input the following information into the notes section:

- The name, date of birth, description, and address of the individual.
- Case numbers and descriptions of paperwork completed on any incidents involving the individual.
- Circumstances of the officer's contact.
- Description of conversations, actions, or conduct of the individual, *e.g.*, threats by the subject against officers, or overt actions to harm officers.
- Location of weapons.
- Reason other than, or in addition to, the above circumstances that would call for caution on the part of other officers contacting this individual, e.g., the residence of the individual is occupied by other potentially dangerous persons.
- Communicable diseases should not be listed; however a notation of "use universal precautions" is acceptable.
- Other medical conditions such as dementia, schizophrenia, etc. may be included in the notes if there is a reliable source of information or documentation. Reliable sources include:
    - Specific advisement from the subject of the alert file or credible and verifiable information from a close relative or guardian of the subject. Statements of this kind must be documented in a police report.
    - Court order, Title 36 petition or a physician's statement attached to or thoroughly documented in a case report.
- A recommendation as to whether the information regarding the individual must be kept in the alert file permanently and the basis for such request.
- A temporary entry of information on an individual may be made when the officer thinks the potential for violence is short term. The officer shall indicate when the information is to be purged: one month, six months, or one year.

The information input into the record shall be reviewed by the inputting officer's immediate or functional supervisor for completeness and approval. Approved records related to mental health and related medical conditions shall be audited by the MHST Unit on a periodic basis.

7130 COMPUTER ENTRIES, CONFIRMATION, CANCELLATION AND TWX

7131 **Computer Entries**

Department personnel who receive or initiate a report of a stolen, impounded, stored, secured at scene vehicle, or stolen, found, stored, or impounded motorcycle, missing person, runaway

juvenile, lost or stolen license plate, or stolen gun shall, within 30 minutes of receiving or initiating the call, contact the TWX operator and provide necessary information for the computer entry.

The TWX operator, upon receiving the information, shall enter it into the computer and printouts of the entry will be incorporated into the case file once the original report is approved and verified by a second TWX operator. The original report will then be forwarded to the TWX operator in Records, who will attach a copy of the computer entry to the report.

When a gun is entered, the operator needs the make, caliber, action and serial number. The weapon cannot be entered into CJIS without all four pieces of information. The TWX operator, upon receiving the information, shall enter it into the computer. The original report will be forwarded to the TWX operator in records, who will attach a copy of the computer entry to the report.

Misdemeanor warrant entries are downloaded from the City Court FACTS system into the TPD Records Management System once a week. Records specialists then enter the misdemeanor warrants into ACIC and attach the printout to the warrant. The warrant documents are filed in the Records Section and confirmation of the warrants is done by contacting personnel in the section.

Records Section personnel will confirm all warrants, stolen vehicles, stolen guns, stolen articles, stolen license plates, missing persons, and runaway juveniles immediately upon request.

7132 **Cancellations**

Department personnel who receive a report of a recovered vehicle (including motorcycles), found person, returned runaway juvenile, found license plate or stolen gun shall contact the TWX operator and determine if the information has been entered into the computer.

If the information has been entered, the TWX operator must clear this data from the computer after being advised to do so by the reporting member. The reporting member shall make an appropriate report under the original case number, indicating that the item or person has been found and is no longer in the computer. The report shall then be forwarded to the TWX operator who shall attach a copy of the computer print data.

If the vehicle, person, license plate or gun has not been entered into the computer, the reporting member shall record this information on the appropriate report. No computer entry will be necessary.

Tucson City Court misdemeanor warrants are cleared from the system once notification of service is received. Members should contact TWX operators when outside agency warrants and felony warrants are served. The TWX operator will handle the locate and follow-up messages on outside agency warrants that are served by TPD officers.

7133 **ALETS/NLETS/ATTEMPT TO LOCATE (ATL) MESSAGES**

Officers requesting a computer message to be sent via Arizona Law Enforcement Telecommunications System (ALETS) or via National Law Enforcement Communications System (NLETS) must specify the region(s) the message will cover, *e.g.*, local only, statewide,

nationwide, or international. Messages sent through ALETS or NLETS or Interpol must meet CJIS requirements. Requests to send messages will only be taken from law enforcement personnel.