82.0 CENTRAL RECORDS

Policy: The Sheriff's Office will maintain a Central Records Unit to retain, archive, and retrieve all law enforcement related operational records, reports, forms and files in an efficient manner and in compliance with governing law.

82.1 Administration

82.1.1 Security and Control

A. Members will not have any original case file/report in their possession unless:

1. The employee is conducting an investigation or follow-up investigation involving the case file/report, or

2. The employee has been summoned to court and the case file/report is necessary for testimony, or

3. The employee has been served with a subpoena duces tecum, (bring with you) or

4. The case file/report is being reviewed by a supervisor prior to being forwarded to the Central Records Unit, or

5. Only agency members shall be in possession of any official Sheriff's Office reports, records, evidence, etc. unless authorized by a member of the Command Staff.

a. In the event a former employee needs any records, reports, evidence etc. for a legitimate purpose, he shall contact his Division Commander and furnish satisfactory proof of the need for the records, reports, or evidence.

b. If the Division Commander is satisfied that the need is legitimate, they may:

1) Authorize the former employee to obtain the needed records, reports, evidence, or

2) Authorize an agency member (sworn or civilian) to accompany the former member to the court hearing or other function and produce the records, reports, or evidence.

3) In this case, the member shall not relinquish custody of the reports, records, or evidence to the former member.

4) Under no circumstances shall any records, reports, evidence be removed from the Records Unit or the Evidence Room without being signed out and accounted for on the proper form(s).

B. Access to Records by Sheriff's Office Staff

1. Normal business hours.

a. The Central Records unit is open Monday through Friday, 0800-1600 hrs, excluding County holidays, or other hours as provided.

1) The Central Records Unit will be secured at all other times and entries in violation of this order are prohibited.

b. Members requesting case files/reports for authorized purposes will submit an "Evidence/Case File Request" to records personnel at least five working days prior to the date the records are needed.

1) Records personnel will not release original case files/reports unless they receive an "Evidence/Case File Request".

c. Members are required to complete and sign the "Report Sign In/Out Log" prior to taking possession of the case files/records and upon return of the case files/records to the Records Unit. Case files/records will be returned within one (1) business day of the court date/trial date.

d. The Records Supervisor or his/her designate shall review the "Report Sign In/Out Log" at least twice per workweek to ensure all records or reports have been returned as stated in this Order.

1) If an employee has not returned case files/records within the approved time frame, the Records Supervisor shall notify that employee's supervisor.

2) The supervisor shall take the appropriate disciplinary action (if warranted by the circumstances).

e. Upon return of the case files/records from a court appearance, the summons/subpoena will be permanently placed in the case file.

2. After normal business hours

a. The Records Room will be locked after normal business hours. All supervisors' issued key fobs will unlock the records room doors. A supervisor may access the Records Room after normal business hours. Only a supervisor will be allowed in the Records Room after hours. Key fobs will not be loaned to other personnel.

b. Any documents (records, warrants, etc.) removed from the Records Room after hours will be logged in accordance with this Order.

C. Public Access to Agency Records - Distribution of Reports controlled by Md. Code, General Provisions Article, Section 4-101 et seq. is governed by section 82.4 below.

D. Expungement

1. Terms

a. "Expungement" means the effective removal of police and court records from public inspection:

1) By obliteration, or

2) By removal to a separate secure area to which persons having no legitimate reason for being there are denied access, or,

3) If effective access to a record can be obtained only by reference to other records, by the expungement of the other records or the part of them providing the access.

b. "Application" means the written request for expungement of police records filed pursuant to the Criminal Procedures Article, Sec. 10-103, and Maryland Rule 4-503.

c. "Notice" means a written request for expungement of police records given a person pursuant to the Criminal Procedures Article, Sec. 10-103, unless the context clearly requires a contrary meaning.

d. "Petition" means a written request for expungement of court and police records filed by a person pursuant to the Criminal Procedures Article, Sec. 10-105(a) and Maryland Rule 4-504.

e. "Police Records" means all official records maintained by a law enforcement agency, a booking facility, or the Central Repository pertaining to the arrest and detention of or further proceeding against an individual for a criminal

charge, a suspected violation of a criminal law, or a violation of the Transportation Article for which a term of imprisonment may be imposed.

"Police records" does not include investigatory files, police work-product records used solely for police investigation purposes, or records pertaining to non incarcerable violations of the vehicle laws of the State or of any other traffic law, ordinance, or regulation.

2. Procedure

a. A person who is arrested, detained, or confined by a law enforcement unit for the suspected commission of a crime and then is released without being charged with the commission of a crime may:

1) Give written notice of these facts to a law enforcement unit that the person believes may have a police record about the matter; and

2) Request the expungement of the police record.

b. Except as provided in paragraph (2) of this subsection, a person may not give notice under this subtitle before the statute of limitations expires for all tort claims that arise from the incident.

1) A person may give notice before the statute of limitations expires if the person attaches to the notice a written general waiver and release, in legal form, of all tort claims that the person has arising from the incident.

2) The notice and waiver are not subject to expungement.

3) The law enforcement unit shall keep the notice and waiver at least until any applicable statute of limitations expires.

4) The person shall give the notice within 8 years after the date of the incident.

c. Upon receipt of a request or Order for Expungement, the Departmental Records Custodian will ensure an attempt is made to verify the facts stated in the notice. If it is determined the facts are true as stated, the Custodian will:

1) Conduct a diligent search for any police records concerning the arrest, detention, or confinement of the person;

2) Within 60 days after receipt of the notice, expunge the police records found concerning the arrest, detention, or confinement; and,

3) Notify the Central Repository and any other law enforcement agency it believes may have police records concerning the arrest, detention, or confinement of the notice and its verification of the facts contained in it. A copy of this notice shall be sent to the person requesting expungement.

3. Denial

When a request for expungement is denied, the law enforcement agency shall notify the person, within 60 days and in writing, of the denial and the reasons for denial. The person may, within 30 days after receipt of the denial, file a petition in the District Court that has venue over the law enforcement agency.

4. Court Ordered Expungement

a. After petitioning the appropriate court and the court determines the order is granted, the Clerk of the Court shall, after 30 days of granting the order for expungement, serve on the Custodian of the Records, two (2) True Test

b. Copies of the Order together with a Certificate of Compliance. Information will be expunged from:

1) Arrest Reports

2) Fingerprint Cards

3) Photographs

4) Criminal History (State & Federal)

5) Criminal Summons

6) Master File

7) Parole/Probation Card

8) Criminal Investigation Report

9) Docket Card

10) Warrant File information

11) Juvenile File

c. The "Certificate of Compliance" will ensure compliance with expungement Court Orders. It will be the responsibility of the Records Custodian of each division in the department to initial, date and indicate if a record was found. All records found will be forwarded to the Patrol Records Custodian for disposition.

d. The original case file and all related documents will be removed from its location in the files to a separate secure area to which the public is denied access, regardless if the case file contains matter relating to multiple defendants, one or more of whom is not entitled to or has not requested expungement, and is required for further proceedings in the action with respect to the other defendants.

e. The original of all files and records ordered to be expunged shall be removed from their filing location and sealed in a manila envelope on which the case file number and a "Certificate of Expungement and Caution" will be attached in such a manner as to seal the envelope. Sealed expungement records may be unsealed on written order of the court or the court may by order, permit access to expunged records in the interest of justice.

1) File index cards, indicating records other than specified in the Court Order, will be removed from the files and a revised card prepared omitting the information relative to the expunged information.

f. A separate alphabetized file index card of persons whose court records have been expunged will be maintained by the Records Custodian. Index cards will contain a reference to the case number of the action or proceeding in which the expungement was ordered.

g. Notices, general waivers, and releases will be maintained by the department in a denied access area until the expiration of any applicable statute of limitation, after which time they may be destroyed by shredding.

5. Storage of Records

All expunged records will be filed and maintained by the Custodian in numerical sequence by case file number, together with the Index of Expunged Records, in a locked filing cabinet to be located on the premises of the Custodian but in a separate area

to which the public/persons having no legitimate reason for access are not allowed.

6. Retention

a. Expunged records will be retained by the Custodian for a minimum of three (3) years. Expunged case files, in multiple defendant cases, shall be retained until the prison terms, if any, of all co-defendants in the action have been served.

b. Upon the expiration of the minimum retention period, and unless otherwise ordered by the court, expunged records, together with the appropriate index card, may be destroyed by the Custodian by shredding or other method of complete destruction.

c. Upon destruction of the expunged records, the name of the person whose records have been destroyed will be deleted from the listing maintained under this section.

7. Disclosure

a. It is unlawful for any person having or acquiring access to an expunged record to open or review it or to disclose to another person any information from it without an Order from the court that ordered the record expunged.

b. Any person in violation, upon conviction, is subject to a fine of not more than $1,000 or imprisonment for one year, or both. If the person is an official of the department, in addition to these penalties, they are subject to dismissal from employment on grounds of misconduct of office.

c. An employer, during an interview or at any other time, cannot require an individual to disclose information concerning criminal charges that have been expunged.

82.1.2 Guidelines dealing with Juvenile Records

A. Dissemination: Dissemination of such information will be tightly controlled and released only for official investigations to members of criminal justice agencies in accordance with Maryland Code, Courts and Judicial Proceedings Article, Section 3-8A-27.

B. Collection: Fingerprints and photos will be taken of juvenile suspects, who are under 18 years of age when arrested or otherwise taken into custody for the commission of a criminal offense, and there is probable cause to believe that the child may have been involved in the commission of that act. Fingerprints may also be taken when a juvenile is suspected of a crime and there are latent prints to send to the Crime Lab for comparison

purposes. Photographs may also be taken for identification purposes when the juvenile is suspected of a crime.

1. If a deputy arrests a juvenile for a criminal offense, he will obtain two complete sets of fingerprint cards from that juvenile offender. The deputy will utilize one WCSO fingerprint card and one State juvenile fingerprint card for that purpose. The arresting deputy will ensure that the following has been completed on both fingerprint cards:
2. At no time will a juvenile taken into custody for a status offense be fingerprinted.

3. The deputy will note the collection of the fingerprints on the arrest report as previously stated in General Order 44. Obtaining other evidence to assist in identification; i.e., blood/hair samples, urine, etc., will be accomplished by court order, unless consent has been obtained from the juvenile and a parent/guardian.

C. Juvenile records will not be filed with adult records, but will be housed in Central Records, and will be kept in a location clearly identifiable from the adult records section. All juvenile records will be clearly marked by Records personnel with the letters "DJS" in red ink for identification as juvenile records. Information in juvenile records will be accessible only to members of criminal justice agencies for investigatory purposes. Information in juvenile records will be unavailable to any parties except with a court order, if ordered sealed by the court in accordance with C.J. 3-8A-27.1.

D. Juvenile records will continue to be house is separate location after the juvenile becomes an adult and will only be accessed as proscribed by law and this order.

E. Expungement of Juvenile Records: Expungement of criminal records are governed by Md. Code, Criminal Procedure Article, Sections 10-101 et seq. (and following) as well as Courts and Judicial Proceedings Article, Section 3-8A-27.1. Any expungements of juvenile criminal records will be in accordance with the foregoing statutes. Also see 82.1.1 D.

82.1.3 Retention Schedule

A copy of the state approved retention schedules will be maintained in Central Records Unit. Each Division Commander and Supervisor is responsible for retaining a copy of the approved retention schedule for their command and for ensuring compliance.

82.1.4 Collection and Submission of Crime Data

A. All incident and arrest report data is maintained in the sheriff's office record management system. Offense classification codes that corelate with

each report is entered into the incident. The offense codes from qualified incidents are submitted for inclusion into the Uniform Crime Report and/or the National Incident-Based Reporting System.

B. At the end of each month, Records personnel will run the computer generated UCR Report and forward it, along with any manually generated supplements, to the Maryland State Police, Central Records in Baltimore, Maryland.

82.1.5 Accounting for Status of Reports

A. Original Report Maintenance – See 42.1.3 Case File Management System

B. Accountability for Conducting Follow Up Reports – See 42.1.4 Accountability for Preliminary and Follow-up Investigations

C. Time Allowed for Submission of Reports

1. Listed below are forms frequently used in reporting and the time frame allowed for submission. Reports covered in other sections of this Manual are not discussed in this Order: i.e., Use of Force Report, Pursuit Report, etc.

a.	Report of Overtime or Court Attendance	2 days
b.	Towed Veh./Veh. Release/Towed Veh. Log	Same day
c.	CIR Initial Report	2 working days
d.	News Release form	Same day
e.	DWI/Alcohol Influence Report	1 day
f.	Arrest/Detention Report	Same day
g.	Missing Person Report	Same day
h.	Accident Report	1 days
i.	Property Held Reports	Same day
j.	Supplement Reports from submission of Initial Report, or the last Supplement Report.	5 days
	1) Supplement reports required for validation purposes will be submitted as directed.	
k.	Equipment Loss/Damage Report	Same day
l.	Animal Bite Reports	1 day

m. Domestic Violence Reports Same day

n. All outstanding reports, not listed above, will be submitted before personnel go on leave of four or more days.

Personnel may seek help from another shift in completing a report; i.e., an animal bite form passed on to another shift to get complete information. It is, however, the responsibility of the initial reporting deputy to follow-up and make sure the report has been completed and submitted.

2. It is the responsibility of the Supervisor to assign those cases, which the original deputy is unable to complete.

82.1.6 Security of Central Records Computer System

A. The Records Management System is backed up on a daily basis. The on-site back-up has security measures in place to deter unauthorized access. The off-site back-up is a downtown data library and also has security measures in place to deter unauthorized access.

B. The Record Management System is virtualized on a local server and can be relocated to any server location, as the situation requires.

C. All access points into the records management system are protected by two layers of password protection.

D. Password Security – the automated system requires a mandatory password change every 120 days to provide for the continued safety of the records system.

82.1.7 Security of Criminal History Records

A. The Department will maintain equipment that will provide access to criminal justice information systems such as the National Crime Information Center, NLETS, and the Maryland METERS System. These systems will provide Criminal History Records.

B. The use of the METERS/NLETS system will be in accordance with rules and regulations of the Sheriff's Office and the controlling authority of the system in use.

C. Messages will be as concise as possible and sent upon the designated authority of this department.

D. All transmissions via METERS/NLETS are to be considered confidential and shall be divulged only to authorized personnel. Sworn and civilian Communications personnel may review messages as received in accordance with the requirements of their work, but such information will only be used within the context of the performance of law enforcement duties.

E. The terminal has the capability of providing a copy of all messages sent and received. The printout can be legally considered probable cause for the arrest of an individual, and is the deputy's best defense against a civil action charging false arrest.

F. The FBI requires all persons with terminal access successfully complete a certification course developed for various levels of access. Personnel with NCIC access must be recertified at least once every two years.

1. Persons not in compliance will have certification revoked and will be required to successfully complete an initial access course prior to being reactivated. Should deactivation occur, the individual involved must contact the departmental Security Coordinator to regain access to the CJIS system.

G. Persons with access to the CJIS system are responsible for password security and information obtained from the various systems using their password. Person assigned a log on ID from CJIS may not share that log on ID with anyone and may not sign onto a terminal for someone else to use.

H. Unauthorized use of log on ID to access any system, or a breach of security procedures related to the use of a log on ID may result in criminal prosecution.

I. The Maryland Department of Public Safety and Correctional Services restrict access to the Maryland Criminal Justice Information Systems to criminal justice employees without significant conviction records. All access to CJIS will be governed by CJIS rules, policies, and regulations.

J. If a member having access is arrested, or indicted, that member will loss their access to CJIS until the charges are disposed of in court. The member will permanently lose access if convicted of any felony or misdemeanor and incarcerated.

82.1.8 CJIS Terminal Agency Coordinator

A. To establish quality control and ensure compliance with State and NCIC policies and regulations, each terminal agency is required to designate an NCIC Terminal Agency Coordinator (TAC). The TAC will be designated by the Sheriff and delegated authority to oversee policy, training, regulations, and operations including, but not limited to:

1. Monthly validations

2. Quality control within the department

3. Assuring all NCIC users are NCIC certified

4. Communications Center Policy Manual distribution

5. ORI assignments

6. Newsletter distribution

7. Liaison with the Maryland Control Terminal Officer (CTO)

8. Coordinate with Maryland and NCIC auditors during departmental audits

9. Act as METERS/NCIC coordinator for the department

10. Submit proper paperwork/documentation to the Public Safety Data Center upon termination of a user's computer access.

B. The TAC will appoint an assistant (ATAC) to assist with duties as outlined in this section. Both the TAC and ATAC, will be required to attend a training session on validations and quality control of terminal operations as such appointments are made, and when such training is available.

82.1.9 CJIS System Security

A. Any member having terminal access, and becoming aware of a breach of a security violation, will notify the Department of Public Safety and Correctional Services Data Security Officer immediately.

1. The member having this knowledge will report the violation either by telephone or in person as soon as possible, followed by a written report within 24 hours. In the absence of the Security Officer, the Security Administrator shall be notified. The written notification shall include:

a. Name of member reporting

b. Name and telephone number of Agency

c. How the problem was discovered

d. A brief description of the problem

e. Estimate of any damage causes

2. The report will be placed in a sealed envelope, marked "personal", and mailed to:

Dean Rohan
Maryland State Police
1201 Reisterstown Road
Pikesville, MD. 21208

3. This matter will be considered confidential and will not be discussed with anyone other than:

   a. The CJIS Security Officer

   b. The employee's immediate supervisor

   c. The departmental TAC or ATAC

   d. The departmental internal affairs investigator

   e. The Sheriff or his designate

4. All personnel are cautioned that the METERS terminal and access to other systems through METERS are specifically provided for use by criminal justice agencies in the pursuit of their lawful duties. No other purpose or intent is permissible.

5. Any request for information received from anyone other than Sheriff's Office personnel will be referred to the Duty Officer.

6. All messages transmitted via the METERS terminal must be logged on appropriate Sheriff's Office forms in accordance with CJIS rules, regulations and policies.

7. METERS regulations direct that each operator is responsible for messages sent by him/her. Therefore, to provide a strict accounting by METERS authorities when audited, each operator will ensure that only official use of the terminal occurs and that accurate records and distribution of the information is established and maintained.

8. CAUTION: Only bona fide queries will be made of criminal history files via the METERS terminal.

9. All members of the department are cautioned that criminal histories are protected by law and if disclosed without good cause, will place the individual procuring the information in jeopardy of civil litigation. Individuals having knowledge their criminal history was queried are entitled to know which department and member made the inquiry. The individual also has the right to confront the agency and agency member to learn the reason for the inquiry.

10. Any employee who violates any CJIS policy is subject to disciplinary action up to and including termination, with the possibility of criminal charges being filed against the violating employee.

82.1.10 Electronic Media Sanitization and Disposal Procedures

DEFINITIONS: Electronic Media: Includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Physical Media: Includes printed documents and imagery that contains Criminal Justice Information (CJI).

A. Electronic media shall be sanitized by overwriting at least three times or degaussed prior to disposal or release to unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Written documentation shall be maintained of the steps taken to sanitize or destroy electronic media. Sanitation or destruction of media shall be witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

82.1.11 Electronic Media Protection Procedures

A. To protect CJI, personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

2. Restrict access to electronic and physical media to authorized individuals.

3. Ensure that only authorized users remove printed form or digital media from the CJI.

4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.

5. Not use personally owned information system to access, process, store, or transmit CJI in violation of established specific terms and conditions for personally owned information system usage.

6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

7. Store all hardcopy CJI printouts maintained by this Agency in a secure area accessible to only those employees whose job

function require them to handle such documents.

8. Safeguard all CJI by this Agency against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.

9. Take appropriate action when in possession of CJI while not in a secure area:

    a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

        i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

        ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.

11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

82.1.12 Electronic Media Transport Procedures

A. Controls shall be in place to protect electronic and physical media

containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or

2. The other agency is performing personnel and appointment functions for criminal justice employment Applicants.

Agency personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

Agency personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.

2. Limiting the collection, disclosure, sharing and use of CJI.

3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.

4. Securing hand carried confidential electronic and paper documents by:

    a. Storing CJI in a locked briefcase or lockbox.

    b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

    c. For hard copy printouts or CJI documents:

i. Package hard copy printouts in such a way as to not have any CJI information viewable.

ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

5. Not taking CJI home or when traveling unless authorized by the LASO (Local Agency Security Officer). When disposing confidential documents, use a shredder.

82.1.13 Physical Protection Procedures

DEFINITION: Physically Secure Location: A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Agency shall be identified with a sign at the entrance.

Visitors Access: A visitor is defined as a person who visits the Agency facility on a temporary basis who is not employed by the Agency and has no unescorted access to the physically secure location within the Agency where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

A. Visitors shall:
   1. Check in before entering a physically secure location by:
      a. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.

b. Document badge number on visitor log if visitor badge issued. If this Agency issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.

c. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.

2. Be accompanied by an Agency escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Show Agency personnel a valid form of photo identification.

4. Follow Agency policy for authorized unescorted access.

a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Agency and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the Agency and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

5. Not be allowed to view screen information mitigating shoulder surfing.

6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

7. Not be allowed to sponsor another visitor.

8. Not enter into a secure area with electronic devices unless approved by the Agency Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the Agency assigned personnel.

9. All requests by groups for tours of the Agency facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

Authorized Physical Access:
Only authorized personnel will have access to physically secure non-public locations. The agency will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.

    a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

    b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

c. Prior to granting access to CJI, the agency on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

d. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.

2. Complete security awareness training.

   a. All authorized agency, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.

   b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.
   a. Take appropriate action to protect all confidential data.
   b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

   a. Report loss of issued keys, proximity cards, etc. to authorized agency personnel.

   b. If the loss occurs after normal business hours, weekends or holidays, personnel are to call the agency POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.

   c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.

5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Web usage—allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency's discretion)

7. Do not use personally owned devices on the agency computers with CJI access. (Agency discretion). See Personally Owned Policy.

8. Use of electronic media is allowed only by authorized agency personnel.

9. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a

non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

10. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.
    a. (Agency Discretion for allowance of CJI via email)
    b. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.
11. Report any physical security incidents to the agency's LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.
12. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis. (See Sanitization and Destruction Policy)
13. Ensure data centers with CJI are physically and logically secure.
14. Keep appropriate agency security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.
15. Not use food or drink around information technology equipment.
16. Know which door to use for proper entry and exit of the agency and only use marked alarmed fire exits in emergency situations.
17. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

Roles and Responsibilities:

Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Agency Coordinator (AC)

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the agency. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security

Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

CJIS System Agency Information Security Officer (CSA ISO)
The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

Information Technology Support
In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the agency by performing the following:

1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the agency. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required agency technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
4. Properly protect the agency's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
    a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
    b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the agency allows the use of personally owned devices. (See the agency Personally Owned Device Policy)
5. Data backup and storage—centralized or decentralized approach.
    a. Perform data backups and take appropriate measures to protect all stored CJI.
    b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.

    c. Ensure any media released from the agency is properly sanitized / destroyed. (See Sanitization and Destruction Policy)
6. Timely application of system patches—part of configuration management.
    a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
    b. When applicable, see the agency Patch Management Policy.
7. Access control measures
    a. Address least privilege and separation of duties.
    b. Enable event logging of:
        i. Successful and unsuccessful system log-on attempts.
        ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
        iii. Successful and unsuccessful attempts to change account passwords.
        iv. Successful and unsuccessful actions by privileged accounts.
        v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
    c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Account Management in coordination with TAC
    a. Agencies shall ensure that all user IDs belong to currently authorized users.
    b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
    c. Authenticate verified users as uniquely identified.
    d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
    e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
    f. Passwords
        i. Be a minimum length of eight (8) characters on all systems.
        ii. Not be a dictionary word or proper name.
        iii. Not be the same as the User-ID.
        iv. Expire within a maximum of 90 calendar days.
        v. Not be identical to the previous ten (10) passwords.
        vi. Not be transmitted in the clear or plaintext outside the secure location.
        vii. Not be displayed when entered.
        viii. Ensure passwords are only reset for authorized user.
9. Network infrastructure protection measures.
    a. Take action to protect CJI-related data from unauthorized public access.
    b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
    c. Enable and update personal firewall on mobile devices as needed.

d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. **Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.*
e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the agency. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

10. Communicate and keep the agency informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to agency.

Front desk and Visitor Sponsoring Personnel
Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the agency personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the agency.
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the agency.
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.
4. Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All agency personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the agency officials. agency, the point of contacts to report any non-secure access is:

82.1.14 User Account-Access Validation Procedures

All accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).

The TAC shall:
- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity (at least once every 6 months), and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

82.2 Field Reporting

82.2.1 Incidents to be Documented by Written Report (Forms to be Used)

A. Guidelines for Reports that must be written

1. The Criminal Investigation Report (CIR) - A CIR will be submitted in, but not limited to, the following instances:

a. Accidental Death: (excluding Motor Vehicle Accident). Photographs may be taken along with other appropriate investigatory actions; i.e., measurements, statements, etc., and included in the report.

The Maryland Occupational Safety and Health Administration (MOSHA) will be notified if the death is industrial in nature, (work related death). A telephone number for MOSHA is available in the Communications Center.

b. Robbery

c. Assault: A CIR will be completed if there is evidence of injury to the victim, or if a weapon was used in the Assault, (whether injury was involved or not), a weapon is to be defined as any article that could inflict bodily harm; i.e., gun, knife, martial arts weapons, club, pipes, etc.

d. Attempted Suicide: Any attempt at self-destruction, or a successful suicide, will be documented on a CIR, and will include the victim's prognosis, if applicable, and the attending physician. Weapons used in suicides or attempts will be confiscated and held until the conclusion of the investigation.

e. Bad Checks:

1) Insufficient Funds: On calls of insufficient fund checks, the victim will be advised to send a registered letter to the subject passing the check, giving ten (10) days for restitution. If restitution is not made, the victim can re-contact this department. A deputy will be assigned and a CIR filed. Warrants will be advised if the identity of the subject passing the check is known. If information is not available for a private warrant, the incident will be investigated to the extent possible.

2) Checks on closed accounts: When a check is passed and the account was closed before issuance of the check, a CIR will be filed. If necessary information is available, private warrants will be advised. If information is not available, the incident will be investigated to the extent possible. In closed account bad checks, charges may be filed without the ten (10) day grace period for restitution.

f. Bigamy

g. Bomb Threats

h. Burglary

i. Conspiracy

j. Child Abandonment

k. Child Abuse/Neglect

l. Confidence Flim/Flam Operations

m. Counterfeiting: A CIR will be done if any action is taken by this Department. Any in-depth investigation of counterfeiting, however, will be referred to, or will be conducted in conjunction with the Secret Service.

o. Damage to Property

p. Controlled Dangerous Substance

q. Extortion

s. False Report of a Crime

t. Forgery

u. Fraud

v. Illegal Gambling

w. Homicide

x. Incest

y. Indecent exposure

z. Kidnapping/Child Abduction

aa. Misuse of Telephone: A CIR will be submitted in the following instances:

1) If the call involves a physical threat.

2) If five or more misuse telephone calls have been received.

3) If the telephone company has determined the origin of the calls and a CIR has not yet been initiated.

bb. Liquor Violations (selling to minors, etc.)

cc. Prostitution

dd. Sexual Offenses

ee. Theft: All reported thefts will be documented on a CIR. If appropriate information is available; i.e., serial number, the item will be entered into NCIC, (reporting deputy's responsibility), and a copy of the printout placed with the CIR.

ff. At any time when ordered by higher authority.

2. Towed Vehicle Reports – shall be written when a motor vehicle is towed at the direction of this department, the following action will be taken by the investigating deputy prior to the end of his tour of duty:

   a. A Towed Motor Vehicle report will be submitted to the Duty Officer. A photocopy of the Towed Motor Vehicle Report will be forwarded to the Records Division.

   b. A Stored Vehicle Release Authorization form will be submitted to the Duty Officer.

   c. The Duty Officer will place the Towed Motor Vehicle report and the Stored Vehicle Release Authorization form in the open folder of the Towed Vehicle Master File, located in the Communications Center. The report number will be placed on the top left margin of the report.

   d. A Certified Copy of Title from the state of last known registration with all lien information will be requested by the towing Deputy.

      1) Immediately upon receipt, the records unit will notify the last registered owner(s) and lienholder(s), if any, that the vehicle was towed and where it is being stored.

   e. Release of Stored Vehicles

      1) Persons wishing to retrieve a vehicle stored by this agency will be directed to the Duty Officer.

      2) Release of a vehicle stored at the direction of this department will require the completion of a Stored Vehicle Release Authorization form indicating the name and address of the person taking possession of the vehicle, date and time of release, and signature of the releasing deputy. Vehicles may be released under the following circumstances:

      3) To the owner if proper identification and proof of ownership is provided.

         To an authorized agent of the owner possessing a notarized form from the owner granting such authorization. Proof of ownership must also be provided.

      4) Upon presentation of a valid Court Order

f. Vehicles stored at the direction of this department will be released only on authority of the storing deputy or higher authority.

g. The second copy of the Stored Vehicle Release Authorization form will be given to the person authorized to take possession of the vehicle. Upon presentation of the Stored Vehicle Release Authorization form to the Tow Service and all fees are paid to the Towing Service, the vehicle may be released.

h. The releasing deputy will submit a supplement report indicating the vehicle has been released. The supplement report, original Towed Motor Vehicle report, and the completed Stored Vehicle Release Authorization form will be forwarded to Central Records.

i. When a Towed Motor Vehicle report is submitted, Central Records will send a Notice To Registered Owner form to the last known owner and any secured parties/lien holders of the vehicle by certified mail, return receipt requested. A copy of this form and the return receipt will be attached to the Towed Motor Vehicle report.

3. Arrest Report: An Arrest Report will be completed in the following instances:

a. Whenever a criminal arrest is made (Statement of Charges).

b. Juvenile Arrests (excluding civil violations).

c. Whenever an arrest is made by warrant. If the subject is apprehended and detained for another agency who actually serves the warrant, the word "Detention" will be underlined at the top of the Arrest/Detention Report, and a copy of the "hit" confirmation teletype of the warrant attached to the Arrest Report.

d. Whenever an "Emergency Petition" is served for a mental evaluation.

e. On any other type of detention where the subject is not free to leave.

f. On services of criminal summons.

4. Motor Vehicle Accident Reports A.C.R.S: (Refer to General Order No: 61.0 - Traffic)

B. Forms to be used for different types of incidents (see above)

C. Information Required in Field Reports – the reports forms are self-explanatory.

D. Procedure to be followed in completing field reports - All blocks must be filled out, if the information in unknown, put unknown. If the information is not applicable, put N/A.

E. Report Accountability**:** On a daily basis, the Midnight Squad Shift Commander will assign each report, from the previous duty day in Keystone, to ensure it is assigned to the appropriate deputy.

1. Each supervisor will review their assigned deputies' report ledger on a weekly basis to ensure all reports and supplements are completed on a timely manner.

2. After all reports are completed they shall be reviewed by the investigating deputy's supervisor. The supervisor will approve the final report and place paper reports in the appropriate in-box in the records copy room. All electronic reports will be forwarded automatically thru Police Mobile to the records department.

82.2.2 Documenting all Incidents in Computer Aided Dispatch System (CAD)

A. The PCO will document all reported incidents though the CAD system that have allegedly occurred in Washington County, which Office has primary jurisdiction over.

1. Citizen reports of crimes

2. Citizen complaints

3. Incidents which deputies are dispatched or assigned

4. Criminal and non-criminal case initiated by law enforcement employees

5. Incidents involving arrests, citations, or summonses

82.2.3 Case Number System – Unique Number for Each Case

Sequential event numbers will be automatically assigned by the CAD System for all initiated activities. Each incident will be given a unique number. In addition, incidents requiring a report will also be assigned a unique report number.

82.2.4 Distribution of Reports and Records

A. Records personnel will distribute records, and reports in accordance with departmental policy and as directed by higher authority. Records and reports to be distributed will include, but not be limited to:

1. Department of Juvenile Services: Offense Reports where a juvenile is charged or arrested will be forwarded to the Dept. of Juvenile Services for disposition.

2. Department of Social Services: Department of Social Services will be sent a copy of all Child Abuse Reports.

3. State's Attorney's Office: Copies of all Offense Reports where an arrest has been made. Copies of all Child Abuse Reports whether an arrest has been made or not. Copies of all Driving While Intoxicated Reports. Copies of all Accident Reports if traffic charges stemmed from the accident.

4. Health Department/Humane Society: Copies of Animal Bite forms.

5. Insurance Companies: Copies as requested of Accident Reports and Offense Reports to insurance companies with defendant information obliterated.

82.2.4 Telephone Report System

A. Certain reports may be taken via telephone as an alternative to dispatching a deputy as follows:

1. Telephone reports may be taken by the Duty Officer, or his designate.

2. Only the following types of complaints may be reported via telephone:

a. Telephone Misuse (may be taken with suspect information if calls received are non-threatening in nature),

b. Vandalism/Destruction of Property (excluding race related/bigot hate crimes),

c. Supplemental reports with a copy to the initial investigating deputy,

d. Certain Motor Vehicle Accidents, when the duty officer will use his discretion during both emergency and non-emergency situations to take pertinent information via telephone, in lieu of deputy responding.

One example of such a situation might be during a severe snowstorm or during icy conditions, when numerous accidents are being reported.

3. A deputy will be dispatched if any of the following factors are present:

a. The incident is in progress, or has just occurred,

b. A suspect is present or location known,

c. There is physical evidence at the scene or the possibility of recovering physical evidence; i.e., prints, witness information, items left by perpetrator, etc.

82.3 Records

82.3.1 Name Index

A. Alphabetical Master Name Index - The Sheriff's Office will maintain an alphabetical master name index. Criteria for inclusion in the name index is met if the names are:

1. Names of victims/complainants

2. Names of suspects

3. Names of accused

4. Locations

82.3.2 Another Indexes or Files

A. The Department will maintain an index of calls for service, and types of crimes.

B. The Department will maintain an index of incidents by location.

C. The Department will maintain an index of stolen, found, recovered, and evidentiary property.

D. The Department will maintain an index of incidents by type.

E. The Department will maintain a Modus Operandi File. As the CIU Supervisor reviews reports, he/she will be alert for Modus Operandi exhibiting unique characteristics that may aid in the identification of known career criminals and in the investigation of certain crimes.

82.3.3 Traffic Records System

A. The Department will maintain a traffic collision data.

B. The Department will maintain traffic enforcement data.

C. The Department will maintain roadway hazard information.

82.3.4 Procedure for maintaining record of traffic citations

A. The Department will maintain a log of citation books issued to deputies.

B. A supervisor shall account for all issued citation books, by initialing the log when a citation book is issued to a deputy.

C. The citation books shall be secured in a locked location.

D. Utilization of E-TIX (Electronic Traffic Information Exchange)

1. The Washington County Sheriff's Office employs E-TIX in its efforts to enforce Maryland Traffic Laws. The Delta+ software was developed and provided free of charge under a license agreement and MOU entered into by the County of Washington and the Maryland State Police as of November 18, 2008. The licensing agreement allows WCSO the use of the software under agreed upon conditions outlined in the licensing agreement. The software was provided free of charge, however any necessary hardware to employ the software is the responsibility of and solely owned by the Washington County Sheriff's Office.

2. The Delta+ system may only be utilized in accordance with MD State Law and with departmental policy to increase efficiency of deputies while conducting traffic enforcement.

a. Operation of Delta+:
   (1) Sworn members of the agency will be assigned and trained in the use of Delta+ software prior to accessing the system for issuance of enforcement related paperwork or other functions.
   (2) Deputies will only log into Delta+ under their user name and password.
   (3) When a Deputy recognizes a motor vehicle infraction he/she will press the button titled "Traffic Enforcement", and if safe to do so input the tag into the pop up screen, if necessary.
   (4) The Deputy will complete the necessary blocks of information to complete the E-Citation, SERO or Warning.
   (5) The Deputy will then issue the operator of the vehicle a copy of the paper work and no signature is required.

b. Voiding an E-TIX Charge(s):
   If a deputy "Submits" a citation in error and determines the citation should be voided, he/she will, within 24 hours;

   (1) Submit a letter of "Request to Void Citation" on departmental letterhead to the Patrol Commander along with a copy of the citation to be voided.

   (2) The Patrol commander will approve/disapprove the voiding of the citation and return the letter and the copy of the citation to the issuing deputy.

   (3) The issuing deputy must then contact the State's Attorney to request a "Nolle Pros" of the citation in District Court.

(4) It is the issuing deputy's responsibility once the citation is "Nolle Prossed", to obtain a copy of the disposition from the District Court.

(5) The issuing deputy must then forward all copies, including the letter to the Patrol Commander, citation, and disposition sheet, to the ETIX Administrator for ECitation deletion.

(6) Once the citation has been deleted from the ECitation system, the ETIX Administrator will attach the confirmation to the void packet and submit all copies to the Patrol Commander for filing.

This entire process should be completed within a two week period.

c. Delta + System out of service:

If the Delta+ system is down for maintenance or out of service, the deputy will revert back to the paper citation, SERO, or Warning until the system comes back up.

d. Race Based Traffic Stop Data Collection:

Maryland Law requires the systematic reporting of data on most traffic stops to the state. Delta+ is set up to report all required data to the state for the participating departments.

82.3.5 Narcotics Task Force (NTF) Records

A. The Narcotics Task Force shall have control all of their records to include:

1. Information Files

2. Open Investigative Files

3. Closed Investigative Files

B. The Narcotics Task Force shall provide to Central Records original copies of arrest reports and charging documents, as well as other supporting documents for all arrests.

82.3.6 Arrestee File

A. The Department will maintain a file on each person arrested to include:

1. Criminal History

2. Fingerprint Card

3. Photograph taken by Patrol Personnel if the subject is released prior to incarceration in the Detention Center, or by Detention Center Personnel if the subject is placed into the Detention Center.

4. Copy of Arrest Report and Charging Documents

B. The first time a subject is arrested by the Sheriff's Office, he/she is assigned a sequential number for a criminal records file. Any subsequent arrests/information concerning that person will be referenced to their sequential number.

C. Each time a person is arrested/charged with criminal charges, the arresting deputy will:

1. Complete an "Arrest/Detention Report". Completing an arrest report after each arrest will assist in updating information on the subject in his/her criminal records file.

2. Central booking will process the defendant.

82.3.7 Internal Affairs Reports

A. Members will not have any original or copies of original internal investigation case files/reports in their possession unless:

1. The employee has been assigned to conduct an internal investigation by the Patrol Commander or higher authority, or

2. The employee has been summoned to court and the case file/report is necessary for testimony, or

3. The employee has been served with a subpoena duces tecum.

a. The subpoena duces tecum will be permanently filed with the original case file/report.

B. Members are not authorized to view internal investigation case files/reports unless:

1. The employee is the subject of the investigation, and

2. The case file/report will be permanently filed with the employee's personnel file and is derogatory in nature.

C. An employee may receive a copy of the case file/report if he is the subject of the investigation and is subject to a hearing board. (Public Safety Article, 3-104)

D. No member will use information or material contained in an official case file/report or an internal investigation to:

1. Commit a criminal act, or

2. Maliciously damage the character, reputation, or integrity of another person

E. Internal Affairs investigations will be filed and maintained in a secure location by the Chief Deputy. Internal investigation files will be retained a minimum of five (5) years past the employee's last day of employment.

82.3.8 File Retention and Secured of Certain Files

A. Personnel files will be maintained in a secure location by the Chief Deputy.

B. Informant files will be maintained in a secure location by the Criminal Investigation Unit Supervisor. Informant files will be retained a minimum of three (3) years past the last date of contact with the informant.

C. The originals of intelligence and vice/organized crime files will be maintained in a secure location by the Criminal Investigation Unit Supervisor. Once an investigation has been completed and the case closed or suspended due to lack of investigatory leads, the file will be placed in Central Records.