7.2 Computers, Electronic Databases, and Information Security

This policy establishes guidelines for the use and security of proprietary and non-proprietary computers and electronic databases to ensure the safeguard of records and other data. It is imperative that the proper protection and access to all criminal justice and motor vehicle files and records is maintained. Protection of information includes, but is not limited to, determining levels of data terminal and physical access, and updating virus detection programs and performing computer scans. This standard assures compliance with administrative and legislative mandates, thus ensuring the effective delivery of the law enforcement services without adverse infringements on personal privacy.

7.2.1 General Information on Computers and Databases

Sheriff's Office computers are to be used only for legitimate law enforcement business. Inclusive in this is the utilization of electronic mail. Software which is not purchased, obtained, or approved by the Office may not be used on any Office computer. Employees shall consider all computer databases or electronic files the property of the Sheriff's Office, unless otherwise designated. Accessed information and other work products shall be treated as confidential information unless such files are specifically approved for public dissemination. Critical information will be accessible to designated or appropriate personnel by physical availability or technology to Office personnel at all times.

The Office will maintain efforts to store critical information, which includes copies of files and programs, on a routine basis at an off-site location. An off-site location must be in a facility other than the one that houses the primary computer files and programs. Critical information is that which, if damaged, lost, or altered, would significantly impede the continued operation or effectiveness of the Office.

The Office's *METERS Security Officer* (who may be sworn or civilian) will insure that there is an ongoing monitoring of accessible criminal justice information systems for verification of all passwords, access codes, and access violations. An annual audit should be conducted to identify recurring or chronic areas of concern.

7.2.2A Use and Dissemination of Criminal History Record Information

Absent prohibitive administrative, executive, or legislative mandates, criminal history information may be released to a requesting public safety organization for a legitimate criminal justice purpose, provided that a "need-to-know" basis has been established by the requesting person or agency. If requested information is considered particularly sensitive, information dissemination approval must be secured from a unit supervisor or administrator prior to release. Unauthorized use of computer systems and/or criminal history record information is strictly prohibited.

7.2.2B Rules for Dissemination of Electronic Information (All Law Enforcement Computer Systems)

All Electronic Information (All Law Enforcement Computer Systems) shall NOT be disseminated to an unauthorized agency, entity, or person. A person shall not access, use, or disclose information from any Law Enforcement Computer System for personal use or gain. Authorized Persons accessing, disseminating and/or receiving any Law Enforcement Computer Systems Information ONLY includes: law enforcement officers, state's attorneys, court commissioners and the courts. Anyone in violation of this order will face disciplinary action.

7.2.3 Physical Security of Files

Files and other official Office documents, to include warrants of arrest, and prisoner and employee background records, will be kept in a secure location under the direct control of supervisory personnel. There are times when records are maintained solely by the affected operational units. In such situations, records maintenance must comply with accepted records retention schedules.

7.2.4 Protection of Information

The Operations Bureau, the Communications Center, and any other area of the Sheriff's Office which has access to Criminal Justice Information System (CJIS) data is considered to be a "Restricted Area." As such, all persons entering or visiting these areas must have successfully completed a background check, including the submission of fingerprints through the Federal Bureau of Investigation. Any visitors or personnel not regularly assigned in these areas (i.e., volunteers, clerks of the court, custodial or maintenance personnel, etc.) and who have not submitted fingerprints through the FBI, must be escorted and/or monitored at all times.

7.2.5 Public Information Act Requests

The following items 1 through 7 are taken directly from Anne Arundel County Administrative Procedures, Department of Law, Effective Date 8/1/2002, published June 30, 2009:

1. PURPOSE

The purpose of this AdminPro is to establish guidelines for the handling of requests made under the Maryland Public Information Act (Maryland State Government Code Annotated §10-611, *et seq.*) (the "PIA").

2. DEFINITIONS

a. APPLICANT - a person requesting to inspect a public record.

b. CUSTODIAN - the Official Custodian or other authorized person who has physical custody and control of a public record.

c. OFFICIAL CUSTODIAN - an officer or employee of the County who is responsible for keeping a public record even if that person does not have physical custody or control of it.

d. PERSON IN INTEREST:

- a person who is the subject of a public record or the designee of that person;
- the parent of a child under the age of 18 years; or
- the legal representative of a person under a legal disability.

e. PIA COORDINATOR - the attorney in the Office of Law assigned to coordinate responses to and provide advice on PIA requests.

f. PUBLIC RECORD - the original or any copy of documentary material that:

1) is made or received by any unit of County government in connection with the transaction of public business;

2) is in any form, including cards, computerized records, correspondence, drawings, film, microfilm, forms, maps, photographs or photostats, recordings, and tape; and

3) includes a document that lists the salary of an employee of the County government.

3. GENERAL REQUIREMENTS

a. All requests for records and other information, in whatever form, including subpoenas, are to be treated as requests under the PIA.

b. Custodians

1) Each Department must designate an Official Custodian and inform the PIA Coordinator of the designation.

2) If there are additional custodians within a Department, the custodians must advise the PIA Coordinator of their names and the records within their custody and control.

3) Each Official Custodian may prepare regulations not inconsistent with this AdminPro as to the handling of requests for certain information within his or her control. Before enforcement, these regulations must be approved by the PIA Coordinator.

4. REQUESTS

a. Other than routine requests, as defined by each Official Custodian in consultation with the PIA Coordinator, each request should be in writing and addressed to the Official Custodian. The request does need not to include a reason, and the applicant should not be questioned as to the reason for the request.

b. The Office of Law has a form that Departments may provide to those who make PIA requests. If any other form is used by a Department, the form must be approved by the PIA Coordinator.

c. The Official Custodian may forward the request to the appropriate custodian for handling.

d. Before allowing or denying access to records, the custodian should confer with the PIA Coordinator unless the PIA Coordinator and the Department have established categories of records to which access may be allowed or denied as a matter of routine without consultation.

e. Each request must sufficiently identify the information requested. If the custodian cannot determine what is being sought, the custodian should ask the applicant to clarify the request.

5. RESPONSES

a. If the request is not submitted to the Official Custodian of the records requested, the Official Custodian, within 10 working days of receipt of the request, must advise the applicant that the records have not been requested from the proper Official Custodian, the identity of the proper Official Custodian, and the possible location of the records sought.

b. If the request will be granted, it must be granted within the reasonable period needed to retrieve the records, but, in any event, within 30 days of receipt. The applicant may agree to a 30-day extension for response.

c. The PIA Coordinator must approve all denials of requests unless the denial falls within an established category of records to which access may be denied as a matter of routine without consultation. Denials must be communicated to the applicant within 30 days of receipt of the request. Within 40 days of the receipt of the request, the applicant must be provided with a written statement giving the reasons for the denial, the legal authority for the denial, and the remedies for the denial.

d. The procedure described in the PIA law for temporary denial may be used only at the direction of and under the guidance of the PIA Coordinator.

e. A custodian does not have to create a requested record.

f. The applicant may be allowed to inspect the requested records or may be provided with copies. The custodian may not allow the applicant to remove original information from the custodian's control for any purpose. If copying facilities are not available, the applicant may hire a copying service to come to the premises where the records are located to make copies on the premises. Under no circumstances may the applicant take the records to be copied.

g. Unless applicable law or regulations provide for a different fee, there is a fee of 25¢ per standard or legal page of copying. Each Official Custodian, with the approval of the PIA Coordinator, may set different fees for larger copies.

h. After the first two hours of search and preparation of records, there is a fee for search and preparation of $20 per hour.

i. A custodian may waive fees below $10. The Official Custodian should consult with the PIA Coordinator before granting any other fee waiver.

6. EXCEPTIONS TO DISCLOSURE

a. Records may not be disclosed if any of these general exceptions apply:

1) an unwarranted invasion of privacy of a person in interest would result from production;

2) the records are privileged or confidential by law; or

3) production is contrary to a State statute, a federal statute or regulation, the rules adopted by the Court of Appeals of Maryland, or an order of a court of record.

b. Examples of records to which access must be denied include:

1) adoption records;

2) welfare records;

3) letters of reference;

4) circulation or other records of a library that contain an individual's name or other identifying information or that identify an individual's use of the library or its materials;

5) library, archival, or museum material contributed on condition that disclosure be limited;

6) retirement records, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-616(g) applies, as determined by the PIA Coordinator;

7) police reports of traffic accidents, criminal charging documents prior to service on the defendant, and traffic citations in the Maryland Automated Traffic System to anyone wanting to inspect the record for purpose of soliciting or marketing legal services who is not the attorney of record for a person named in the record;

8) personnel records of an individual, except to the person in interest or an elected or appointing official who supervises the work of the subject of the record;

9) hospital records relating to medical administration, staff, medical care, or other medical information containing general or specific information about one or more individuals;

10) student records, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-616(k) applies, as determined by the PIA Coordinator;

11) recorded images from traffic control signal monitoring systems, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-616(o) applies, as determined by the PIA Coordinator;

12) Motor Vehicle Administration records containing personal information (defined as address, driver's license number, medical information, name, photograph, social security number, telephone number), unless one of the exceptions to denial in Maryland State Government Code Annotated §10-616(p) applies, as determined by the PIA Coordinator;

13) records pertaining to arrest warrants, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-616(q) applies, as determined by the PIA Coordinator;

c. Examples of information that must be redacted from any records being produced include:

1) medical and psychological information, except that the person in interest may inspect as permitted under Maryland Health General Code Annotated §4-304(a);

2) sociological information, as defined by an Official Custodian's regulations (**Although there is no general prohibition on disclosing personal information, there is a prohibition on releasing sociological information. The Anne Arundel County Sheriff's Office defines sociological information as: information that identifies an individual including an individual's address, driver's license number or any other identification number, medical or disability information, name, photograph, or computer generated image, Social Security number, or telephone number. The official custodian of Anne Arundel County Sheriff's Office records shall deny inspection of the part of a public record that contains sociological information. Such sociological information may be redacted in accordance with SG § 10-617 (Advice of Counsel, Office of the Attorney General, October 14, 2009);**

3) after consultation with the person who or the representative of the entity that provided the information, and in consultation with the PIA Coordinator, trade secrets, confidential commercial or financial information, and confidential geological and geophysical information;

4) the home address or telephone number of a public employee, unless the employee gives permission or the Department employing the individual determines, in consultation with the PIA Coordinator, that production is in the public interest;

5) other than the salary of a public employee and except to the person in interest, financial information relating to an individual;

6) security for information systems;

7) licensing records in an occupation or profession, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-617(h) applies, as determined by the PIA Coordinator;

d. Examples of information for which access may be denied, after consultation with the PIA Coordinator, if disclosure is contrary to the public interest, include:

1) inter-agency and intra-agency documents that would not be available in litigation;

2) testing records for academic, licensing, or employment examinations, except that, after a promotional exam is taken and scored, a person in interest may inspect the test and the results but may not make a copy of the exam;

3) specific details of a research project that an institution of the State or a political subdivision is conducting, except for the name, title, expenditures, and date when the final summary will be available;

4) a real estate appraisal made for a public agency about a pending acquisition, except to the owner of the property;

5) law enforcement agency's records of investigation, intelligence information, security procedures, or investigatory files, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-618(f) applies, as determined by the PIA Coordinator;

6) site specific location of certain plants, animals, or property, unless one of the exceptions to denial in Maryland State Government Code Annotated §10-618(g) applies, as determined by the PIA Coordinator;

7) to the extent that production would jeopardize the security of a structure owned by the State or any of its political subdivisions, would facilitate a terrorist attack, or would endanger the life or physical safety of an individual:

i) response procedures or plans prepared to prevent or respond to emergency situations, disclosure of which would reveal vulnerability assessments or specific tactics, emergency procedures, or security procedures;

ii) building plans, blueprints, schematic drawings, diagrams, operational manuals, or other records of airports, mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums, and waste and water systems, disclosure of which reveal the building's or structure's internal layout, specific location, life, safety, and support systems, structural elements, surveillance techniques, alarm or security systems or technologies, operational and transportation plans or protocols, or personnel deployments; and

iii) records prepared to prevent or respond to emergency situations identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories established, maintained, or regulated by the State or any of its political subdivisions.

7. RESOURCES

a. Custodians should use The Public Information Act Manual published by the Office of the Maryland Attorney General as a guide to responding to PIA requests. It is available through the Office of Law or on the internet at www.oag.state.md.us/Opengov/index.htm.

7.2.6 Covert Investigations (**Freedom of Association & Assembly Protection Act of 2009**)

Public Safety Article, § 3-701(m) requires that "on or before January 1, 2010, each law enforcement agency other than the [Maryland State Police] shall adopt a written, publicly available policy governing: (1) the conduct by the agency of covert investigations of persons, groups, or organizations engaged in First Amendment activities; and (2) each agency collection, dissemination, retention, database inclusion, purging, and auditing of intelligence information relating to persons, groups, or organizations engaged in First Amendment Activities." The regulations found at the 28 Code of Federal Regulations (C.F.R.), part 23 apply to "all criminal intelligence systems portaging through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3711, *et seq.*

Definition

In this policy, "covert investigation" means a surreptitious infiltration of or attempt to infiltrate a group or organization for the purpose of interfering with the group's activities that involve freedom of speech or association, the exercise of religion, freedom of the press, or the right to petition the government activities that may be protected by the First Amendment to the United States Constitution.

This policy does not apply to surreptitious or undercover investigations that do not involve protected First Amendment activities.

Authorization to conduct Covert Investigations

The members of this agency shall not conduct a covert investigation of a person, group, or an organization involved in First Amendment activities, to the extent such activities are known to be protected, without the express written authorization of the Sheriff or his/her designee. The Sheriff or designee will authorize the investigation only if the investigation is justified because:

1. There is reasonable, articulable suspicion that the person, group, or organization is planning or is engaged in criminal activity; and

2. A less intrusive means of investigation is not likely to yield satisfactory results.

Mere membership or participation in a group or organization engaged in First Amendment activities does not alone constitute reasonable, articulable suspicion of criminal activity (see also 28 C.F.R. § 23.20(c) defining reasonable suspicion or "criminal predicate.").

If the Sheriff is unable to give prior authorization of the covert investigation, he/she shall, as soon as is practicable afterwards, make a written finding that the conditions

above existed and justified the covert investigation (see 28 C.F.R. § 23.30(c) requiring accountability of the "head of the government agency").

Any covert investigation shall be done only for legitimate law enforcement objectives with a due regard for safeguarding the applicable constitutional rights and liberties of all persons who may be affected by the investigation. In every case, the least intrusive investigative methods should be used.

The investigation shall conclude when all logical leads related to criminal activity have been exhausted, or when no legitimate law enforcement objective justifies continuing the investigation (See 28 C.F.R. § 23.20(a)).

Collection, Retention, and Dissemination of Collected Information

To the extent that investigators engaged in a covert investigation collect information solely about the political beliefs, ideologies, and association of the individuals, group, or organization, the investigators shall not retain or maintain any such information unless:

1. The information is relevant to a criminal investigation; or

2. There is reasonable, articulable suspicion that the person, group, or organization advocates, supports or encourages the violation of any federal, State or local criminal law that prohibits acts of terrorism, racketeering activity (as defined by 18 U.S.C. § 1961), violence, extortion, destruction of property, intimidation, harassment, obstruction of justice, or fraud (See 28 C.F.R. § 23.20(c)).

Information entered into and maintained in a criminal intelligence file or database shall be evaluated for the reliability of the source of the information and the validity and accuracy of the information. If information is maintained in a computer database, that information shall be classified in a manner that clearly reflects the purpose for which the information has been collected and maintained, particularly information about a specific individual, group, or organization that is suspected of engaging in specific crime(s). See 28 C.F.R § 23.20(g) & (h).

Such records may be disseminated only in accordance with existing agency procedures, including but not limited to those based on the Maryland Public Information Act, Maryland Annotated Code, State Government Article § 10-601 *et seq.* and 28 C.F.R. § 23.3 (b)(3). The database shall be reviewed annually, beginning on January 1, 2011, and any information that has become moot, irrelevant, or is otherwise without law enforcement value shall be purged from the database.