Security of Criminal Justice Information System

.01 Policy

The policy of the Bladensburg Police Department is that all computer systems and record documents will be accessed and used only for criminal justice and law enforcement purposes. Computer screens, program functions, sign on codes and passwords, screen layouts and format, computer and record information will not be accessed, viewed, or shared with non-law enforcement personnel without proper authorization, i.e., Security Service Agreements.

All persons who access Bladensburg Police Department data, records and criminal justice information system(s) must comply with specifications set forth by all governing bodies, including but not limited to the Criminal Justice Information System Security Policy, the Maryland Electronic Telecommunications Enforcement Resource System (METERS) policy, federal and state law, and any other governing entity.

Data stored on the law enforcement network or external media that is law enforcement related and is documented criminal justice information must be protected to ensure correct, legal, and efficient dissemination and use. Any individual receiving a request for criminal justice information must ensure the person requesting the information is authorized to receive the data. Stored data on the law enforcement network or external media is sensitive and should be treated accordingly. An unauthorized request or receipt of law enforcement information or CJIS data could result in criminal proceedings or interdepartmental disciplinary action for any infraction, violation, or misuse of the system.

.02 Terms

Law Enforcement Information System: an assembly of computer hardware, firmware, and software configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Criminal History Record Information (CHRI): is arrest-based data and any derivative information from that record, i.e., descriptive data, FBI number, conviction status, sentencing data, incarceration, probation and parole information.

Confidential Information: information maintained by state agencies that is exempt from disclosure under the provisions of the Public Information Act or other applicable state or federal laws. The controlling factor for confidential information is dissemination. Criminal History Record Information (CHRI) is protected by Federal legislation.

Data Security Coordinator(DSC): the person designated to administer the Control Terminal Agency's information security program. The DSC is the agency's internal and external point of contact for all information security matters. and shall ensure that each local agency having access to a criminal justice network have a security point-of-contact.

Noncriminal justice purpose: the uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Physical Security: (1) The measures used to provide physical protection of resources against deliberate and accidental threats. (2) The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and accidental damage.

Information Security: is the result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Hacking: unauthorized use or attempts to circumvent or bypass the security mechanisms of an information system or network.

.03 Governing Legislation and Reference

Governing Legislation:

Criminal Justice Information Systems, 28 CFR 20.

Maryland Code, §10-201, et seq.

Maryland Regulations, COMAR 12.15.01, .02, .03.

Department of Justice v. Reporters Committee, 489 U.S. 749, 764 (1989).

Forms: N/A

.04 Procedure

The Chief of Police will designate a Data Security Coordinator (DSC) who shall have the general responsibility for managing the physical and electronic security structure of the law enforcement information system. The SC will report directly to the Chief of Police for matters relating to the criminal justice information system. Specific responsibilities of the SC include, but are not limited to the following:

- Identify who has access to the Bladensburg Police Department law enforcement information system and who is using electronic hardware and software for the specific purpose of ensuring that no unauthorized users have access to the system;
- Conduct criminal background screening and fingerprint checks (federal and state) on all personnel. Personnel that have a criminal record shall not have access to criminal justice information;
- Ensure each person who is authorized to store, process, and/or transmit criminal justice information and CJIS data is individually identified by use of a unique identifier. A unique identification shall also be required for all persons who administer and maintain the system(s) that access the criminal justice information system and network;
- Require signed User Agreements prior to authorization or access to the Bladensburg Police Department criminal justice information system by allied law enforcement personnel;
- Provide physical security for Bladensburg Police Department criminal justice information system and network to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed or stored data;
- Ensure that security awareness training is provided at least once every two (2) years to all employees/authorized users (within six months of a new hire, appointment, or assignment) who manage or have access to the Bladensburg Police Department criminal justice information system and CJIS data. Training shall meet the standards of Maryland CJIS policy;
- Ensure that a complete topological drawing which depicts the interconnectivity of the Bladensburg Police Department's system configuration is maintained in a current status. The words "FOR OFFICIAL USE ONLY" shall appear near the bottom of the page containing the drawing; and,
- Support policy compliance and keep the Chief of Police informed of security incidents.

Criminal justice information, data, and resources available to Bladensburg Police Department employees or authorized users and accessed through all information systems or electronic media are to be used for official use to further the goals and objectives of the Bladensburg Police Department by providing an effective method to:

- Communicate;
- Perform research;
- Complete reports; and,
- Obtain information while performing law enforcement related tasks.

Employees and authorized users of the Bladensburg Police Department criminal justice information system are expected to use good judgment while using any and all computer related resources, information systems and electronic media. Employees and authorized users are to abide by the following:

- All software licensing agreements and restrictions;
- User agreements between the employee/authorized user and the Bladensburg Police Department;
- Requirements set forth by Maryland CJIS and National Crime Information Center (NCIC) Security Policy; and,
- All applicable security requirements set forth by the Bladensburg Police Department, State and Federal Agencies and approved service providers.

The unauthorized use of computer, electronic media, and information systems containing Bladensburg Police Department law enforcement information and CJIS data for unofficial purposes is a violation of Bladensburg Police Department

policy and CJIS Security Policy. Unauthorized and unofficial activities which create violations include, but are not limited to, the following:

- Using any information system to include any type of computer or server without proper authorization;
- Assisting in, encouraging, or concealing from the Bladensburg Police Department or other authorities any unauthorized use, or attempted unauthorized use, of any information system to include any type of computer or server;
- Knowingly endangering the security of any criminal justice information system, computer, or server, or willfully interfering with others authorized for usage of these systems;
- Giving away or sharing any password assigned to them to access any criminal justice information;
- Reading, altering, or deleting any other person's files or electronic mail without specific authorization;
- Downloading or introducing unauthorized programs or files;
- Manipulating or altering current software on Bladensburg Police Department mobile or desktop computer(s);
- Transmitting any material or messages in violation of Federal, State, local law or Town policy, including sexually, racially, or ethnically offensive comments, jokes, slurs, threats, harassment, slanders, or defamation;
- Accessing or distributing obscene or suggestive images or offensive graphical images;
- Distributing sensitive or confidential law enforcement information;
- Distributing unauthorized broadcast messages or solicitations;
- Using Bladensburg Police Department provided electronic media to accomplish personal gain or to manage a business;
- Distributing copyrighted materials not owned by the Bladensburg Police Department, including software, photographs, or any other media;
- Downloading copyrighted information or software;
- Developing or distributing programs designed to infiltrate computer systems internally or externally;
- Accessing or downloading any resource for which there is a fee without prior, appropriate approval;
- Attempting to access any system an employee is not authorized to access (hacking);
- Listening to voice mail or reading electronic mail of another employee; or,
- Endorsing political activities.

Violations of this General Order or CJIS Security Policy may result in disciplinary action up to and including dismissal and criminal prosecution.

HISTORY: Adopted February 28, 2013

This General Order supersedes all other orders and memoranda in conflict therewith.

Authority:

Charles L. Owens
Chief of Police