CJIS Access, Maintenance, and Security

805.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use, maintenance, and security of department systems that access Criminal Justice Information.

805.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal Justice Information (CJI) - Data provided by FBI Criminal Justice Information Services (CJIS) that is necessary for law enforcement agencies to perform their mission and enforce the laws (e.g., biometric, identity history, person, organization, case/incident history data).

Security incident - Any incident that compromises the security of CJI or systems that access CJI. Examples include but are not limited to unauthorized use of legitimate code or credentials within department systems, email communications that contain malicious code, data breaches, signaling to external systems, and unauthorized exporting of information.

805.2 POLICY

It is the policy of the Havre de Grace Police Department to maintain the security, confidentiality, and integrity of its information systems that access CJI by collaborating with appropriate state and federal agencies to implement the applicable established protocols.

805.3 CJIS COORDINATOR

The Chief of Police shall appoint a CJIS coordinator, who shall be responsible for the Havre de Grace Police Department's adherence to FBI CJIS Security Policy requirements.

The CJIS coordinator shall establish procedures necessary to govern the department's use, maintenance, and security of systems that access CJI as described in this policy.

805.3.1 CJIS COORDINATOR RESPONSIBILITIES

The responsibilities of the CJIS coordinator include but are not limited to:

(a) Coordinating with others, such as the information technology or legal departments, as appropriate, to maintain department compliance with FBI CJIS Security Policy requirements and the Maryland Department of Public Safety and Correctional Services' Information Technology and Communications Division.

(b) Managing member accounts with access to CJI, including:

1. Creating, enabling, modifying, disabling, and removing member accounts in accordance with this policy and the FBI CJIS Security Policy.
2. Configuring member accounts in accordance with federal and state requirements (e.g., limiting unsuccessful login attempts).
3. Reviewing member accounts for compliance with legal and policy requirements at least annually.

(c) Overseeing the maintenance, repair, and replacement of CJI systems and system components in accordance with manufacturer or vendor specifications and/or department requirements, including:

1. Maintaining a list of organizations and personnel approved by the Chief of Police to perform maintenance on CJI systems.
2. Approving, scheduling, documenting, and monitoring all maintenance and diagnostic activities, whether performed on-site, remotely, or off-site, and maintaining records.
3. Verifying that non-escorted personnel performing maintenance on any CJI system or terminal possess the required access authorizations, and designating members who have the required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
4. Maintaining records for all system maintenance and diagnostic activities.

(d) Monitoring department systems that have access to CJI to ensure compliance with applicable laws and this policy; developing processes to detect, identify, and correct flaws in software and firmware; and conducting security updates as necessary.

(e) Providing for the security of hardware that includes provisions for the following:

1. How hardware is to be brought into and taken out of department facilities
2. Physical security of hardware within department facilities
3. Physical security of areas containing network connections and transmission lines, including monitored access

(f) Implementing and carrying out the department Incident Response Plan, including:

1. Tracking and documenting all suspected or actual security incidents related to CJI in an appropriate manner.
2. Directing annual testing of the department's information security incident response capabilities using tabletop or walk-through exercises, simulations, or other types of testing.
3. Making the appropriate notifications outside of the Department (see the Records Maintenance and Release Policy for additional guidance).
4. Providing information on security incidents to any third-party software developers or vendors as appropriate.

(g) Protecting digital and non-digital media that contain CJI, including physical security, transportation, destruction/sanitization, and documentation requirements.

(h) Developing and updating department information security and privacy literacy training and incident response training as required by policy.

(i) Maintaining audit records in accordance with the established records retention schedule, but in no event for less than one year.

(j) Managing the development, documentation, and dissemination of procedures for the following:

1. Awareness and training
2. Incident response
3. Audit and accountability
4. Access control
5. Identification and authentication
6. Configuration management
7. Media protection
8. Physical and environmental protection
9. System and communications protection
10. System and information integrity
11. Maintenance
12. Security and privacy planning
13. Contingency planning
14. Risk assessment

(k) Reviewing this policy and related procedures as required by the FBI CJIS Security Policy and proposing updates as needed to the Chief of Police.

805.4 MEMBER RESPONSIBILITIES

All members of the Department shall be committed to detecting information security incidents and making the appropriate notifications.

Any member who suspects that there may have been unauthorized access, disclosure, or other compromise of CJI shall report their suspicions in accordance with the Incident Response Plan within one hour of the discovery.

Personally owned devices or systems and publicly accessible systems shall not be used to access, process, store, or transmit CJI.

805.5 SUPERVISOR RESPONSIBILITIES

Supervisors shall notify the CJIS coordinator when the account access of a member they supervise needs to be modified, disabled, or removed for any reason, such as resignation, termination, or change of duties.

805.6 MEMBER ACCOUNTS

Department accounts used to access CJI shall only be created upon approval of the Chief of Police or the authorized designee.

Member accounts shall be disabled within one week of any of the following:

(a) The account has expired.

(b) The account is no longer associated with a member.

(c) The account is found to be in violation of this policy.

(d) The account has been inactive for 90 calendar days.

If any threat to the confidentiality, integrity, or availability of CJI related to a specific member account is detected, the CJIS coordinator or designated member shall disable the account within 30 minutes of the discovery.

805.6.1 ACCESS AUTHORIZATION

Access authorization for systems transmitting, receiving, using, or storing CJI shall be based on the principle of least privilege as follows:

(a) Members shall only be granted access authorizations that are necessary to accomplish assigned department tasks.

(b) Accounts with security privileges shall only be authorized for members with an operational need for the privileges. Privileged functions shall be logged as they are executed.

(c) Non-privileged members shall not be allowed to execute privileged functions.

805.6.2 ACCOUNT REVIEW ACTIVITIES

At least annually, the CJIS coordinator shall review member accounts for compliance with policy and applicable laws. The CJIS coordinator shall validate account privileges and remove or reassign them as necessary to accurately reflect the department mission and law enforcement needs.

805.7 MEDIA PROTECTION

Access to media containing CJI shall be restricted to authorized members and stored within physically secured locations or controlled areas, in accordance with the FBI CJIS Security Policy.

Digital media (e.g., flash drives, external or removable hard disk drives, compact discs) containing CJI shall be encrypted. Personally owned digital media devices or digital media devices with no identifiable owner shall not be used on department systems that store, process, or transmit CJI.

Non-digital media (e.g., paper files, printed pages, microfilm) containing CJI should be enclosed in an opaque folder or container if they are to be transported outside of physically secure locations or controlled areas. Media containing CJI shall not be left unattended outside of a physically secure location.

Transportation and transfers of media containing CJI shall be documented.

805.7.1 MEDIA DISPOSAL AND RELEASE

Digital media containing CJI shall be overwritten at least three times or degaussed (i.e., erased) prior to being disposed of, released from department control, or released for reuse. Inoperable digital media devices, such as hard drives or solid-state drives that cannot be accessed to

overwrite the data, shall be physically destroyed. When non-digital media is no longer needed for investigative or security purposes, it shall be destroyed by crosscut shredding or incineration.

805.8 SYSTEM AND INFORMATION INTEGRITY

The integrity of department CJI systems shall be protected through the implementation of appropriate controls such as:

(a) Flaw remediation.

(b) System monitoring.

(c) Security alerts, advisories, and directives.

(d) Software, firmware, and information integrity controls.

(e) Spam protection.

805.9 INCIDENT RESPONSE PLAN

[Insert your agency's Incident Response Plan consistent with CJIS 5.3 IR-4, IR-7, and IR-8 – see the Guide Sheet for additional guidance.]

805.10 SECURITY AWARENESS TRAINING

Members with physical or electronic access to CJI or CJI systems shall complete security awareness training appropriate to their assigned roles and responsibilities and shall certify their understanding by signing a formal Security Awareness Training Acknowledgement. Training shall include information security and privacy literacy training, security incident response training, and a review of this policy and related procedures.

Security awareness training shall be completed prior to accessing any CJI data or system and at least annually thereafter. Additional training shall be completed as required following any changes to CJI systems and for any member involved in a security incident within 30 days of the event.

Individual training records shall be maintained in accordance with the established records retention schedule, but in no event for less than three years.

The department's CJIS training shall be reviewed for any necessary updates or changes annually and following any security incident or change in a CJI system or the FBI CJIS Security Policy.

805.11 SANCTIONS

Failure to adhere to policies and procedures pertaining to CJI shall result in disciplinary action, up to and including termination. Misuse of or failure to secure CJI may also result in temporary or permanent restrictions in the use of CJI. Intentional misuse of CJI may also be prosecutable under applicable laws.