Protected Information

703.1 VERSION

Review Date	Effective Date	Approving Authority
02/02/19	07/09/18	Eric D. English, Chief of Police

703.2 POLICY AND PURPOSE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Harrisonburg Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

Employees of the Harrisonburg Police Department will adhere to all applicable laws, orders, regulations, user agreements and training related to the access, use, dissemination and release of protected information. For procedures related to this policy, please refer to Maintenance and Release of Criminal History, DMV, and Incident Reports Supplemental policy.

703.3 ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this policy. Responsibility rests with the supervisor to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated. This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

703.4 DEFINITIONS

Protected information - Any information or data that is collected, stored or accessed by employees of the Harrisonburg Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

703.5 RESPONSIBILITIES

The Chief of Police shall select a member of the Department to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS) and Department of Motor Vehicles (DMV) records.

(b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information (Virginia Code §9.1-130; Virginia Code §19.2-389; Virginia Code §19.2-389.1; 6 VAC 20-120-50; 6 VAC 20-120-60).

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

703.6 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Harrisonburg Police Department policy or training. Only those employees who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the employee has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a employee to administrative action and/or criminal prosecution.

703.7 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

An employee who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Unit to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department employees or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

703.7.1 REVIEW OF CRIMINAL HISTORY RECORD

A person whose criminal history record is maintained by this department has the right to inspect a copy of his/her information at the Department for the purpose of ascertaining the completeness and accuracy of the information. For offenses that are required to be reported to the Central Criminal Records Exchange (CCRE), the requester shall be referred to the CCRE. For offenses that are non-reportable to CCRE, the Department shall provide the information requested following the dissemination procedures as required by 6 VAC 20-120-50 (Virginia Code §9.1-132).

703.8 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select an employee of the Department to oversee the security of protected information.

The responsibilities of this position include, but are not limited to:

(a) Developing and maintaining security practices, procedures and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.

(d) Tracking, documenting and reporting all breach of security incidents to the Chief of Police and appropriate authorities.

703.8.1 EMPLOYEE RESPONSIBILITIES

Employees accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle, in an unlocked desk drawer or file cabinet, on an unattended computer terminal).