Protected Information

703.1 VERSION

Review Date	Effective Date	Approving Authority
10/14/2021	07/09/2018	Kelley Warner, 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 an employee 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 an employee of the Department to coordinate the use of protected information.

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

(a) Ensuring employee 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 (Va. Code § 9.1-130; Va. Code § 19.2-389; Va. Code § 19.2-389.1; Va. Code § 38.2-613(B)(5); 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.

703.5.1 NCIC/VCIN PROCEDURES

All VCIN/NCIC procedures will be performed according to the rules and regulations covered in the VCIN and NCIC Operating Manuals and Code Manuals. These manuals should be referred to when questions arise pertaining to VCIN or NCIC matters. The manuals will be kept updated by the Terminal Agency Coordinator (TAC) or as assigned.

The Harrisonburg Police Department has adopted the FBI CJIS Security Policy as our security policy. In addition, regarding misuse of information received from the VCIN/NCIC systems, our agency will follow the guidelines as shown in the System Section of the VCIN Operations Manual.

(a) Disciplinary Guidelines for Misuse of NCIC/VCIN

(b) System Operation Rules and Procedures

1. System Security
2. Penalties for Unlawful Actions

In the event of a security incident where the security of the VCIN/NCIC system or access to the system is breached or there is a concern of such, our agency will follow the procedures as outlined in the CJIS Security Policy. This includes notifying the Virginia State Police VCIN Section of any misuse or security incidents involving the VCIN/NCIC System.

703.5.2 VCIN COMPUTER SANITIZATION POLICY

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at the Harrisonburg Police Department. These rules are in place to protect sensitive and classified information derived from the VCIN/NCIC system. Inappropriate disposal of media may put employees and the agency at risk.

This policy applies to all Harrisonburg Police Department employees, contractors, and temporary staff who have access to VCIN/NCIC systems, media, or data. This policy applies to all equipment that processes, stores, and/or transmits VCIN/NCIC data.

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, printouts, and other similar items used to process, store and/or transmit VCIN/NCIC data shall be properly disposed of in accordance with measures established by the Harrisonburg Police Department. An authorized employee of the Harrisonburg Police Department will complete the sanitization process.

Physical media (printouts) shall be disposed of by shredding. Electronic media (hard-drives, tape cartridges, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the following methods:

(a) Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

(b) Degaussing - a method used to magnetically erase data from magnetic media.

(c) Destruction - a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be retrieved.

Systems that have been used to process, store, or transmit VCIN/NCIC data shall not be released until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

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.

703.6.1 COMPUTER SECURITY INCIDENT

A computer security incident can range from a simple virus to the disclosure of sensitive information. Incidents can be minor or major and can be either intentional or accidental. Activities that must be reported include both internal and external security incidents.

Examples of such incidents include:

- Loss, theft, or missing data, equipment, or IT resources
- Denial of Services (DoS) intentional or unintentional
- Compromise of computer security (includes virus and malware threats)
- Phishing attempts to acquire sensitive information such as usernames or passwords for malicious reasons, by masquerading as trustworthy in an electronic communication

- Unauthorized access to the VCIN/NCIC system or data

All employees and users are required to immediately report any suspicious incidents involving the security of the VCIN/NCIC System. Incidents must be reported to TAC/LASO or designee and must include the following information:

Brief description of events:

(a) What happened

(b) Where it happened (console ID)

(c) When did it happen (date and time)

(d) Possible cause of incident, if known

(e) Immediate action taken

Additional information Roles and Responsibilities:

If VCIN/NCIC data is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

(a) Employees shall notify their supervisor or TAC/LASO immediately. The report must contain a detailed account of the incident, events leading to the incident, and steps taken in response to the incident.

(b) If reported to a supervisor, the supervisor shall notify the TAC/LASO of the event as soon as possible.

(c) The TAC/LASO or designee will begin an internal investigation with the assistance of the IT department/company if necessary and will notify the VSP VCIN Section of all security incidents.

703.6.2 VCIN/NCIC PHYSICAL SECURITY POLICY

Access to the computer system hardware, software and media are physically protected through the above mentioned access control measures. All personnel (employees, maintenance staff, I.T. staff, janitorial staff, etc.) who have access to secure areas have completed CJIS Security Awareness Training and have passed an FBI fingerprint based background check. All visitors will be escorted by an authorized person and will not be allowed access to the VCIN/NCIC System, CJIS Information derived from VCIN/NCIC, or to any other confidential information.

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).