802.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following:

(a) Requests for inspection of records may be submitted verbally or written including by facsimile or electronic mail (NMSA § 14-2-7; NMSA § 14-2-8).

1. Written requests shall include the name, address, and phone number of the person seeking access to the records and shall identify the records sought with reasonable particularity. No individual requesting records shall be required to state the reason for inspecting the records.

(b) The Department is not required to create records that do not exist (NMSA § 14-2-8).

(c) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released as provided in NMSA § 14-2-9.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/ video release should be maintained in the department-approved media storage system, and a notation should be made in the case file to document the release and the reasons for the redacted portions.

(d) Copies of records shall be provided in the same medium, electronic or paper, in which the request was made in addition to any other medium that is appropriate (NMSA § 14-2-7; NMSA § 14-2-9).

(e) Inspection of records shall be permitted immediately or as soon as practicable, but no later than 15 days after receiving a written request (NMSA § 14-2-8).

1. If the inspection is not permitted within three business days, the Records Manager shall provide a written explanation of when the records will be available for inspection or when the Records Manager will respond to the request. The three-day period shall not begin until the written request is delivered to the office of the Records Manager.

(f) If it is determined that the record request is excessively burdensome or broad, an additional reasonable period of time shall be allowed. The Records Manager shall provide written notification to the requester within 15 days of receipt of the written request for the need of additional time (NMSA § 14-2-10).

(g) If the Department is not in possession or has the responsibility of the records requested, the Records Manager shall promptly forward the request to the custodian of the requested public records, if known, and notify the requester (NMSA § 14-2-8).

1. The notification shall state the reason for the absence of the records from the Department, the records location, and the name and address of the custodian.

802.4.2 DENIALS

If a written request is denied, the Records Manager shall provide the requester with a written explanation of the denial. The denial shall describe the records sought, the name and titles or

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department

positions of each person responsible for the denial, and be delivered or mailed to the requester within 15 days after the written request for inspection was received (NMSA § 14-2-11).

802.4.3 REQUESTS FOR VIDEO OR AUDIO

A request for release of video or audio shall specify at least one of the following (NMSA § 14-2-1.2):

(a) The computer-aided dispatch record number

(b) The police report number

(c) The date or date range with reasonable specificity and at least one of the following:

1. The name of the officer
2. The approximate time
3. The approximate location
4. Other criteria established and published by the Department to facilitate access to videos

802.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Any personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver's license record, motor vehicle record, or any department record, including traffic accident reports, is restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Personal identifier information (NMSA § 14-2-1.1; NMSA § 14-2-6).

(c) Prior to charges filed, name, addresses, contact information, or protected personal identifier information of victims of or non-law enforcement witnesses of alleged crimes as provided in NMSA § 14-2-1.2.

(d) Prior to charges filed, name, addresses, contact information, or protected personal identifier information of individuals who are accused but not charged with a crime (NMSA § 14-2-1.2).

(e) Visual depiction of a deceased person, depictions of great bodily harm, or acts of severe violence resulting in great bodily harm unless caused by a law enforcement officer as described in NMSA § 14-2-1.2.

(f) Visual depiction of an individual's intimate body parts as described in NMSA § 14-2-1.2.

(g) Visual or audio depiction of the notification to a member of the public of a family member's death (NMSA § 14-2-1.2).

(h) Confidential sources, methods, or information (NMSA § 14-2-1.2).

(i) Records pertaining to a physical or mental examination and medical treatment of individuals unless the information could be relevant to a criminal investigation or an

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department

investigation of misfeasance, malfeasance, or other suspected violation of law as provided in NMSA § 14-2-1.2.

(j) Attorney-client privilege information (NMSA § 14-2-1).

(k) Information closed to the public pursuant to the Abuse and Neglect Act (NMSA § 32A-4-1 et seq.).

(l) Adult abuse records except where allowed by law (NMSA § 27-7-29).

(m) Tactical response plans or procedures prepared for or by the state of New Mexico or a political subdivision of the state (NMSA § 14-2-1).

(n) Information relating to an applicant or to a licensee of a concealed handgun license except as allowed by law (NMSA § 29-19-6).

(o) Records related to the investigation of a missing person or unidentified human remains (see the Missing Persons Policy for additional guidance) (10.2.5.1 NMAC et seq.).

(p) Automated license plate reader data (Driver Privacy and Safety Act, S.B. 40, 57th Legislative Session - Second Session, § 3 (2026)).

(q) Any other information that may be appropriately denied by state or federal law.

802.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Records Manager for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, Village Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

802.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

Each audio/video recording released should include the department name and to whom the record was released.

802.8 EXPUNGEMENT

Expungement orders received by the Department shall be reviewed for appropriate action by the Records Manager. The Records Manager shall expunge such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once a record is expunged, members shall respond to any inquiry as though the record did not exist (NMSA § 29-3A-5; NMSA § 29-3A-7).

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department

Protected Information

803.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release, and security of protected information by members of the Village of Cuba 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.

803.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored, or accessed by members of the Village of Cuba 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.

803.2 POLICY

Members of the Village of Cuba Police Department will adhere to all applicable laws, orders, regulations, use agreements, and training related to the access, use, dissemination, and release of protected information.

803.3 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), Motor Vehicle Division (MVD) records, and Law Enforcement Data System (LEDS)/New Mexico Law Enforcement Telecommunications System (NMLETS).

(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. See the Village of Cuba Police Department CJIS Access, Maintenance, and Security Policy for additional guidance.

(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.

(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.

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department

803.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Village of Cuba Police Department policy, or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member 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 member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

803.5 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.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Manager 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 Section 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 members, or the public is at risk.

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

803.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the Department to oversee the security of protected information.

The responsibilities of this position include but are not limited to (see the CJIS Access, Maintenance, and Security Policy for additional guidance):

(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.

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department

(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.

803.6.1 MEMBER RESPONSIBILITIES

Members 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).

803.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

Copyright Lexipol, LLC 2026/09/21, All Rights Reserved.
Published with permission by Village of Cuba Police Department