NEW MEXICO LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM AND THE NATIONAL CRIME INFORMATION CENTER MEMORANDUM OF UNDERSTANDING BETWEEN THE NEW MEXICO DEPARTMENT OF PUBLIC SAFETY AND

Agency: Santa Fe County Adult Detention Facility

This agreement is made and entered into the 18th day of March 2026 through the 31st day of December 2026 by and between the New Mexico Department of Public Safety (hereinafter referred to as DPS) and Originating Agency Identifier (ORI): a criminal justice and/or law enforcement agency (hereinafter referred to as USER AGENCY). The DPS serves as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) in New Mexico for the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) and is the supervisory agency for the New Mexico Criminal Justice Information System (NMCJIS), NCIC Criminal History Interstate Identification Index (III), and all other Criminal Justice Information System (CJIS)-related systems including New Mexico Law Enforcement Telecommunications System (NMLETS). The International Public Safety and Justice Network (NLETS), a long-standing non-governmental organization, facilitates New Mexico Law Enforcement Telecommunications System (NMLETS) services in New Mexico.

Whereas, because DPS serves as the State agency responsible for the management and operation of the above services, the purpose of this agreement is to govern the exchange of, and responsibility for, the information shared between the DPS Systems and the USER AGENCY. The DPS will facilitate local law enforcement and other criminal justice agencies' requests to participate in the information services provided on the DPS network as long as the USER AGENCY abides by applicable federal and state laws, regulations, policies, and procedures related to these systems.

The DPS maintains and operates the NMLETS computer system under shared management pursuant to this User Agreement. A Terminal Agency Coordinator (referred to hereafter as the "TAC") shall be designated for each USER AGENCY and is responsible for that Agency's use, security, and personnel. All parties will operate in accordance with New Mexico and Federal law. This Agreement shall be governed, construed, and enforced in accordance with the laws of the State of New Mexico. This User Agreement shall not be amended; any revision will require a new version of this agreement to be approved by the DPS and signed by all parties.

SECTION 1: NMLETS/NMCJIS

THIS SECTION APPLIES TO ONLY NMLETS TERMINAL AGENCIES.

1.1 DUTIES OF THE DPS: Upon receipt of inquiries from the USER AGENCY which contain all the data elements required by the NMLETS/NMCJIS and NCIC Systems, the DPS agrees to furnish the USER AGENCY such criminal justice information as is available through the NMLETS, and further agrees to furnish record information as is available and authorized from the FBI/NCIC System. The DPS agrees to incorporate the necessary rules and regulations of the State of New Mexico, the Federal Government, NCIC, NLETS, and NMLETS/NMCJIS Operating Manuals into training as necessary, and to provide specialized training on such rules and regulations to the USER AGENCY TAC on at least an annual basis.

The DPS further agrees to provide NMLETS operational and Hit Confirmation support to the USER AGENCY. The DPS will maintain an automated log of all hot file and III transactions as prescribed in the FBI CJIS Security Policy. These documents are available in the DPS CJIS Web Portal. If USER AGENCY accesses NMLETS and is unable to access this portal, please submit a ticket via the Help Center at https://help.dps.nm.gov requesting a Virtual Private Network (VPN).

1.2 DUTIES OF THE USER AGENCY: The USER AGENCY will collect, receive, store, use, and disseminate all information covered by the terms of this agreement in strict compliance with all present and future Federal and State laws and regulations, and with all rules, procedures, and policies adopted by the DPS as described in the NCIC, NLETS, and NMLETS/NMCJIS Operating Manuals, and the FBI CJIS Security Policy. The NMLETS/NMCJIS system is restricted to serving the informational needs of governmental criminal justice agencies and others specifically authorized by law.

The USER AGENCY will familiarize its personnel who ultimately use information received via NMLETS/NMCJIS with the (NLETS) Rules, Policy, and other operating or dissemination instructions as are found in the NCIC, NLETS, and NMLETS/NMCJIS Operating Manuals, and the FBI CJIS Security Policy.

The USER AGENCY further agrees to restrict the use of NMLETS/NMCJIS to those legitimate purposes described in the NCIC, NLETS, and NMLETS/NMCJIS Operating Manuals, and the FBI CJIS Security Policy, and agrees not to provide information received via NMLETS/NMCJIS to any other agency or person who is not covered by a valid and current agency user agreement with NMLETS/NMCJIS except as may be provided by law.

i. **Incident Reporting and Information Sharing**
   The User Agency agrees to comply with the CJIS Systems Agency (CSA) incident reporting requirements and procedures for all cybersecurity incidents that impact, or have the potential to impact, the confidentiality, integrity, or availability of the Agency's networks, systems, applications, or infrastructure connected to, supporting, or capable of storing, processing, or transmitting Criminal Justice Information (CJI).

ii. **Reporting Timeframe**
   Per CJIS Security Policy (IR-6), all suspected incidents must be reported immediately—and no later than one (1) hour after discovery—to DPS CJIS Systems Agency (CSA). Agencies must follow the CSA Incident Reporting Phone Tree until a live contact is reached.

iii. **Reportable Incidents**
   a. Security events – suspicious network activity, phishing/malicious emails, malware.
   b. Breach events – unauthorized access or compromise of CJI or Personally Identifiable Information (PII).
   c. Supply chain events – counterfeit or malicious hardware/software.
   d. Physical events – loss/theft of CJI devices or unauthorized physical access.

iv. **Indicators of Compromise (IOCs)**
   Agencies will provide known indicators of compromise to the CSA as promptly as operationally feasible to enable timely detection and assessment of potential impacts within the CSA's

environment.

v. **Incident Response Summary**
Following containment and recovery, agencies will submit a comprehensive incident report to the CSA. This report must include:

a. A description of the incident and timeline of events,
b. Steps taken to contain and remediate the issue,
c. Detailed remediation and environment-hardening measures implemented, and
d. A complete list of identified IOCs.

The USER AGENCY acknowledges that these requirements are designed to ensure timely detection, containment, and coordinated response across the CJIS community. Detailed procedures, including immediate action steps and the CSA Incident Reporting Phone Tree, are published separately by NMDPS and must be adhered to in full.

ALL Cybersecurity reports are CONFIDENTIAL – IMMEDIATE REPORTING IS CRITICAL TO PROTECT THE STATE AND CJIS NETWORKS.

Under New Mexico's Inspection of Public Records Act (IPRA) (NMSA 1978, §14-2-1(A)(7)), records that could expose security vulnerabilities—such as tactical plans or cybersecurity reports—are exempt from disclosure to protect public safety and prevent potential terrorist or cyberattacks.

Accordingly, the cybersecurity reports are considered confidential and are exempt from disclosure under this provision, as their release could compromise public safety and security.

1.3 DATA SHARING: The USER AGENCY is responsible and accountable for ensuring that any contractors/vendors they contract with that utilize NCIC and NMLETS/NMCJIS data will share data with DPS, in a timely manner, for common purposes as defined by DPS.

1.4 ACCOUNTABILITY AROUND DATA SHARING: The USER AGENCY has sole responsibility and accountability for ensuring compliance with all laws, regulations, policies, and procedures applicable to its entry and sharing of information including, but not limited to, the federal Driver's Privacy Protection Act (18 U.S.C. §2721 et seq.) as well as any and all applicable New Mexico State laws pertaining to records and data.

1.5 EXECUTORY CLAUSE: It is understood by and between the parties hereto that the DPS is obligated to provide services described in Section 1.1 above to the USER AGENCY, and the USER AGENCY is obligated to provide information to DPS as described in Section 1.2.

1.6 DUTIES OF THE TAC: The USER AGENCY will designate an individual to serve as the TAC who shall be responsible for ensuring compliance with NMLETS/NMCJIS and NCIC policy and regulations, including all duties outlined in the NCIC TAC Handbook. The TAC will work directly with the New Mexico CJIS Systems Officer (CSO) or designee on all matters dealing with NMLETS/NMCJIS. Each Agency shall provide at least one trained secondary TAC to serve in the primary TAC's absence.

Duties of the TAC include, but are not limited, to:

i. Maintaining the most current versions of the CJIS Security Policy, NMLETS/NMCJIS Operating Manual, and NCIC Operating Manual and making them available to the appropriate personnel;
ii. Ensuring all staff are provided with training adequate for their responsibilities, duties, and degree of CJIS Systems access or use;
iii. Appropriately managing operator access to CJIS Systems to include determining appropriate access, managing account password reset and submitting a request with the user access form to DPS to terminate access immediately upon separation of the employee;
iv. Disseminating essential system-related bulletins as needed to relevant agency personnel;
v. Reporting any allegation or finding of misuse of CJIS information by agency personnel to the DPS;
vi. The TAC shall be responsible for ensuring adequate training for operators within the agency;
vii. Being the main point of contact for the CJIS audits; and
viii. Completing monthly Validations through the DPS identified system.

1.7 DUTIES OF ORGANIZATIONAL PERSONNEL WITH SECURITY RESPONSIBILITIES (OPSR, previously known as the Local Agency Security Officer (LASO)):

The USER AGENCY will designate an individual to serve as the Organizational Person with Information Security and Privacy Responsibilities (OPSR) who shall be responsible for ensuring compliance with NMLETS/NMCJIS and the CJIS Security Policy. The OSPR will serve as the primary technical liaison between the local agency, CJIS CSA, and the FBI. This role is critical in ensuring compliance with the CJIS Security Policy and supporting the agency in maintaining the necessary technical infrastructure and documentation.

The individual selected as the OPSR for the USER AGENCY shall be identified on the final page of this document. Any changes to this designation must be communicated within ten (10) working days to the NCIC Coordinator for the DPS, via the Help Center at https://help.dps.nm.gov or dps.ncic-support@dps.nm.gov or calling 505.827.3413.

The Criminal Justice Agency's Chief Security Authority (CSA) acknowledges that, in certain agencies, the Terminal Agency Coordinator (TAC) and the OPSR roles may be performed by the same individual. However, the agency and individual are still responsible for ensuring that all duties and responsibilities outlined for each role in the current FBI CJIS Security Policy are fulfilled in accordance with policy requirements.

Duties of the OSPR include, but are not limited, to:

i. Maintaining the most current version of the CJIS Security Policy and making it available to the appropriate personnel.
ii. This individual and the Agency Head are also responsible for enforcing the policy at the Agency;
iii. Identifying and documenting how their Agency interface is connected to the State system (Network Diagram);
iv. Ensuring that personnel security screening procedures are followed as stated in this policy;
v. Ensuring that the approved and appropriate security measures are in place and working as expected;
vi. Serving as the technical point of contact for the CSA (DPS) and the FBI, and assisting with

technical audit questions, clarifications, and updates;

vii. Supporting policy compliance and ensuring the NM Information Security Officer (ISO) is promptly informed of all security incidents where CJI may be affected;

viii. Assisting in preparing for, and responding to, audits by the FBI and DPS, and ensuring all technical requirements and documentation are accurate and up to date; and

ix. Advising the Agency on industry best practices to enhance the security and compliance of systems handling CJI data.

x. Technical Liaison: Serving as the technical point of contact for the CSA (DPS) and the FBI, and assisting with technical audit questions, clarifications, and updates.

xi. Creating and maintaining:

a. Network Diagram Management: Assisting in creating, maintaining, and updating the Agency's network diagram in accordance with most current CJIS Security Policy.

b. Physical Diagram Management: Assisting in creating, maintaining, and updating the Agency's physical diagram in accordance with most current CJIS Security Policy.

c. CJIS Security Policy Compliance: Helping the Agency implement and maintain the technical controls required by the CJIS Security Policy to ensure secure handling and transmission of Criminal Justice Information (CJI).

1.9 PRIORITY 1 CONTROLS: The USER AGENCY shall ensure that Priority 1 Controls are in place in accordance with the current version of the CJIS Security Policy. Failure to comply with these controls may result in sanctions.

1.10 HIT CONFIRMATION: The USER AGENCY shall ensure that the Hit Confirmation procedures, as prescribed in the NCIC, NLETS, and NMLETS/NMCJIS Operating Manuals, are adhered to.

1.11 HOURS OF OPERATION: All USER AGENCIES with file entry capabilities on NMLETS/NMCJIS are required to maintain twenty-four (24)-hour, seven (7)-day-a-week operation. USER AGENCIES not operating twenty-four (24) hours a day, seven (7) days a week are required to enter into an agreement with a USER AGENCY that operates twenty-four (24) hours a day, seven (7) days a week to act as its alternate terminal as prescribed in the NMLETS/NMCJIS Operating Manual.

1.12 QUALITY CONTROL: The Agency Administrator/Agency Designated Administrator and/or the appointed Terminal Agency Coordinator (TAC) accepts responsibility for the timely entry and the validity of all records entered by the USER AGENCY. The individual selected as the TAC for the USER AGENCY must be identified on the final page of this document, further noting that any changes to this designation must be communicated within ten (10) working days to the NCIC Coordinator for the DPS, at dps.ncic-support@dps.nm.gov, via the Help Center at https://help.dps.nm.gov, or by calling 505.827.3413. Procedures for timely entry and the validation process are outlined in the NCIC and NMLETS/NMCJIS Operating Manuals. Measures for purging or canceling entries will be adhered to in order to maintain system integrity. The USER AGENCY must fully comply with quality control and Hit Confirmation procedures or risk removal of records from NCIC/NMCIC and possible loss of connectivity to NMLETS/NMCJIS.

1.13 DATA DISSEMINATION: The USER AGENCY shall record all disseminations of Criminal History Record Information (CHRI) received via NMLETS/NMCJIS on the prescribed log. The log shall be maintained and retained for at least three (3) years from the date of the transaction. Criminal history requests through the III must be in accordance with current III policies and procedures. The USER

AGENCY must ensure that CHRI received will only be used for those purposes for which it was provided. In addition, all data retrieved from NMLETS will adhere to dissemination regulations outlined in the NMLETS Operating Manual.

SECTION 2: TECHNICAL AND SECURITY

THIS SECTION APPLIES TO ALL AGENCIES THAT UTILIZE THE DPS NETWORK.

2.1 DUTIES OF THE DPS: The DPS will provide seven (7) days-a-week technical support specialists. From 0000 to 0800 it will only provide "emergency support," which includes any event that affects the ability of an officer or a dispatch center to perform their job function. The DPS will provide after-hours technical support. Through these mechanisms, the DPS will provide support to verify that the connectivity to the DPS network is operational.

The DPS will be responsible for:

i. Providing application software to the USER AGENCY that supports the intent of this agreement and connectivity to the DPS.
ii. Answering questions and troubleshooting issues directly associated with the applications the DPS provides. These applications include, but may not be limited to, NMLETS and CJIS.
iii. Working with the USER AGENCY to design and implement internet working solutions that are both secure and mutually beneficial to each agency's processes and working with the USER AGENCY to provide knowledge transfer for the implemented technologies.
iv. Storing and creating audit logs with information about events that occurred on the DPS firewall, DPS host systems, or DPS network.
v. Notifying USER AGENCY of update schedules, system requirements, recommended standards, etc.

The DPS will **NOT** be responsible for:

i. Non-DPS supported software and/or applications.
ii. Non-DPS hardware components such as PCs, printers, switches, routers, firewalls, wiring, etc.
iii. PC Operating Systems.
iv. Initial and ongoing maintenance (patches, updates, etc.) on any and all of the above.
v. USER AGENCY system and network logs.

2.2 DUTIES OF THE USER AGENCY: The USER AGENCY hereby agrees that the USER AGENCY is responsible for all initial, recurring, and replacement costs and support associated with connectivity to the DPS network, including but not limited to PCs, routers, circuits, and printers, and is responsible for all initial, recurring, and replacement costs and support associated with additional security measures recommended by the DPS which are required in the FBI CJIS Security Policy. To protect these services, any suspected compromise of USER AGENCY network shall be reported to the DPS immediately upon recognition of the suspected compromise so that DPS can report the compromise to the

FBI in thirty (30) minutes or less. USER AGENCY **MUST** immediately call 505-629-1221 or 505-303-4746 upon discovery and continue to report until its issue has been acknowledged. Compromise includes any credible network threat, breach, attempted breach, cyberthreats, etc.

The USER AGENCY understands, agrees, and accepts that the USER AGENCY is responsible for all PC support, which includes loading and set-up of the DPS application software as provided. The USER AGENCY will notify the DPS at least five (5) business days prior to adding and/or replacing any existing workstations with access to NMLETS. The USER AGENCY is responsible for implementing and maintaining virus protection software on local network devices. The USER AGENCY must comply with Multi-Factor Authentication requirements. The USER AGENCY's hardware and software must comply with current NIST standards. The USER AGENCY devices that are connected to the DPS network shall use the DPS-provided station name.The USER AGENCY shall be removed from the network in the event of failure to comply with these requirements.

The USER AGENCY shall request in writing to the DPS at nm-cso@dps.nm.gov and receive written approval for any new computer-aided dispatch, records management systems, connections, circuits, and/or any other systems that process, store, or transmit any criminal justice information, as well as any modifications to those currently existing prior to the USER AGENCY entering into any contracts or ordering any such item from a vendor. Any USER AGENCY with connectivity to another organization's network and/or the Internet shall implement the security technologies outlined in the NMLETS Operating Manual. Along with the implementation of security technologies, the USER AGENCY must provide DPS with, or cooperate with DPS personnel to create, documentation of these links to external connections. All internetworking solutions to be implemented on networks with connectivity to the DPS must also be submitted in writing and receive written approval by DPS prior to the USER AGENCY entering into any contracts or supplying funds for such solutions. All submissions referenced in this paragraph are subject to approval by the DPS to ensure compliance with security laws, regulations, and policies. The USER AGENCY shall ensure that all vendor/contractor personnel are properly vetted prior to gaining access to CJI according to the current version of the CJIS Security Policy (CJISSECPOL).

2.3 PERSONNEL SECURITY: The USER AGENCY will ensure that prior to gaining access to Criminal Justice Information (CJI), all personnel will be screened according to the personnel background screening policy prescribed in the current version of the FBI CJIS Security Policy. State and National fingerprint-based background checks shall be required pursuant to the CJIS Security Policy for all agency personnel and contractors with direct, indirect, or incidental access to CJI (including but not limited to: maintenance staff, IT staff, HR staff, and those with direct read/write system access) prior to gaining access to CJI. If any records are returned from the background check, access will not be granted until the CJIS Systems Officer (CSO) or his/her designee can review the matter to decide if access/employment is appropriate. In addition, NCIC Criminal History (III), NCIC, and NMLETS wants and warrants checks will be conducted prior to employment. If a felony conviction of any kind is found, access will not be granted. All personnel must undergo a fingerprint-based background check every five (5) years and have a III run annually. Completed background check records must be retained and made available for audits.

The USER AGENCY must also provide the proper role-based security and literacy training to personnel depending upon their access to CJI. This training **must** be given prior to gaining access to NMLETS information, and completed annually, when system changes are made, when security incidents occur, when changes are made to the CJIS Security Policy, and following any DPS and/or local agency audits.

2.4 TRAINING OF PERSONNEL: The USER AGENCY personnel operating NMLETS terminals, including Mobile Data Terminals/Computers (MDTs/MDCs), are required to satisfactorily complete the prescribed training as provided by or approved by the DPS. The USER AGENCY TAC is responsible for ensuring initial training, functional testing, and affirming the proficiency of terminal operators within ninety (90) days of employment or assignment. They must also ensure that in-service retraining, functional retesting, and reaffirmation of the proficiency of terminal operators are provided annually in order to ensure compliance with NCIC and NMLETS policies and regulations. The training provided should focus on entry level training on the use of any software used to access NMLETS, NCIC Criminal History (III) requirements and record quality for criminal justice agency records personnel.

2.5 OPERATOR ACCESS: The USER AGENCY is responsible for actions of agency personnel using the NMLETS system and data derived from the NMLETS system. All systems submitting or receiving CJI, Criminal History Record Information (CHRI), or Personally Identifiable Information (PII) shall uniquely identify each user. Any violation of the policies incorporated in this agreement shall be prohibited by the agency, including but not limited to:

i. Sharing of user credentials for access to the NMLETS System;
ii. Allowing NMLETS access from publicly accessible computers.

Each agency shall set standards of discipline for the violation of CJIS policies and document such standards. This may include incorporating the handling of violations of CJIS policy into agency policies for other disciplinary actions, up to and including USER AGENCY employee access suspension.

2.5 DATA SHARING: The USER AGENCY is responsible and accountable for ensuring that any vendor/contractor that utilized NCIC and NMLETS data meets the requirements in this agreement. The USER AGENCY and any vendors/contractors will share data with DPS in a timely manner for common purposes as defined by DPS.

2.6 ACCOUNTABILITY AROUND DATA SHARING: The USER AGENCY has sole responsibility and accountability for ensuring compliance with all laws, regulations, policies, and procedures applicable to its entry and sharing of information including but not limited to the federal Driver's Privacy Protection Act (18 U.S.C. §2721 et seq.) as well as any and all applicable New Mexico State laws pertaining to records and data.

2.7 SECURITY: The USER AGENCY agrees to limit access to information furnished by NMLETS to authorized employees, contractors/vendors, and other criminal justice/law enforcement agencies who have entered into this agreement with the DPS and/or the USER AGENCY to protect the security and privacy of this information.

2.8 AUDITS: The USER AGENCY will allow terminal access to State and Federal Auditors to conduct audits of the agency and contractors/vendors, as prescribed in the NCIC and NMLETS Operating Manuals and the FBI CJIS Security Policy. The DPS will conduct an audit for each agency at least once every three (3) years. Additionally, the FBI audit staff will conduct audits at least once every three (3) years, which will include a sample of criminal justice agencies in New Mexico that are authorized recipients of CJI. The objective of this compliance audit is to verify adherence to DPS and FBI policies and regulations.

The USER AGENCY TAC is the primary point of contact for audit information. Audit information requested for DPS or FBI auditing purposes is to be provided in a complete and timely manner. The OPSR shall provide technology security audit information through the TAC.

2.9 SANCTIONS FOR VIOLATIONS: The DPS may sanction the USER AGENCY for failure to meet the standards of the policies referenced in this document. If a DPS audit identifies policy violations, the DPS will report the findings to the agency in violation and request a mitigation plan. Failure to mitigate audit findings will result in sanctions as directed by the DPS.

The DPS may impose sanctions on individual operators if an operator is found to have used DPS-CJIS systems in a manner that is against FBI and/or DPS policy, whether for unauthorized access, improper dissemination, unfounded query, or other use of the system that is not pursuant to state or federal laws. These sanctions may include corrective training, temporary suspension, or permanent revocation of access.

2.10 ACCESS RESTRICTIONS TO NCIC AND CRIMINAL HISTORY RECORD INFORMATION

National Crime Information Center (NCIC) and Criminal History Record Information (CHRI) systems contain highly sensitive criminal justice information and are governed by federal law and the CJIS Security Policy. Access is not discretionary and must be granted strictly in accordance with policy based on role and function.

Access to NCIC and CHRI is limited by the following authorities:

i. CJIS Security Policy Version 6.0:

a. Information Handling: Access to CJI must be restricted to authorized individuals. *See* generally, CJISSECPOL, V. 6.0, Access Control, as amended.

b. Access Control Policy: Agencies must implement technical and procedural controls to enforce the principle of least privilege. *See* CJISSECPOL, v. 6.0, AC-6, as amended.

c. Personnel Security: Only individuals who have undergone appropriate background checks may be granted access to unencrypted CJI. *See* CJISSECPOL, V. 6.0, Personnel Security, PS-3, as amended.

d. Security Awareness Training: Users must complete appropriate training prior to being granted access and annually thereafter. *See* CJISSECPOL, V. 6.0, AT-2, as amended.

e. Outsourcing Standards: Vendors with access to CJI must operate under management control of a CJA and sign an MCA and a Security Addendum. *See* CJISSECPOL, V. 6.0, Appendices D. and H, as amended.

ii. 28 CFR Part 20 – Criminal Justice Information Systems:

a. § 20.21(b)(1): CHRI shall only be made available to criminal justice agencies for criminal justice purposes.

b. § 20.25: CHRI may only be accessed or disseminated for authorized uses; misuse or unauthorized access constitutes a violation of federal regulation. Any agency or individual violating subpart B of the regulations [related to CHRI] shall be subject to a civil penalty not to exceed the civil penalty amount as provided in 28 CFR 85.5. The current penalty is $36,498.

iii. NCIC Operating Manual:

a. Access is granted solely based on operational necessity under the "right to know" and "need to know" standard.

b. Any use outside of official duty (e.g., curiosity or convenience) is considered misuse and may result in disciplinary action or loss of system access.

iv. Implications of Unauthorized Access:

a. Audit findings or corrective action from the FBI CJIS Division or NMDPS as the state CSA

b. Sanctions including temporary suspension of access

c. Civil and criminal penalties for misuse of federal databases

2.11 EFFECTIVE DATE, TERMINATION, AND EXPIRATION

This Agreement is effective when signed by the Parties, by and through their duly authorized representatives, and shall remain in effect until terminated as hereinafter set forth. Either Party may terminate this Agreement for any reason. The terminating party must provide the non-terminating party with written notice of termination at least thirty (30) days in advance. Either Party may immediately terminate this Agreement without advance written notice if either party, including any of its officers, employees, agents, and any other persons associated with either Party, violates any applicable state or federal law, rule, regulation, procedure, or policy. If access is no longer needed or authorized by applicable state or federal law, rule, regulation, procedure, or policy, the USER AGENCY must immediately notify the New Mexico Department of Public Safety to terminate access. The New Mexico Department of Public Safety may immediately terminate USER AGENCY access when an applicable state or federal law, rule, regulation, procedure, or policy no longer allows for USER AGENCY access. This agreement expires on December 31st each year, and new agreements shall be completed annually or within ten (10) calendar days of the date of a change in the signatories.

2.12 MERGER

This Agreement is the complete and exclusive statement of the agreement between the Parties with respect to the subject matter thereof and supersedes all prior negotiations, representations, proposals and other communications between the Parties, either oral or written. The Agreement may only be amended by a written document signed by the Parties by and through their duly authorized representatives.

SECTION 4: USER AGENCY INFORMATION AND ROLE DESIGNATION

I. USER AGENCY INORMATION		
Agency Name: Santa Fe County Adult Detention		
Agency Physical Address: 28 Camino Justica	City Santa Fe	
Address Line 2	Zip 87508	State N.M.
FBI Originating Agency Identifier (ORI): NM026065C		
II. TERMINAL AGENCY COORDINATOR		
Full Name and Title Emeterio Chavez Admissions & Release Records Manager		
Email Address Epchavez@santafecountynm.gov	Phone Number (505)428-3843	
III. ASSISTANT TERMINAL AGENCY COORDINATOR		
Full Name and Title Armando Trujillo CQI		
Email Address artrujillo@santafecountynm.gov	Phone Number (505)428-3229	
IV. ORGANIZATIONAL PERSONNEL WITH SECURITY RESPONSIBILITIES (OPSR)		
Full Name and Title Dominic LeDoux		
Email Address DLeDoux@santafecountynm.gov	Phone Number (505)428-3112	
V. USER AGENCY HEAD		
Full Name and Title Gregory S. Shaffer, Santa Fe County Manager		
Email Address gshaffer@santafecountynm.gov	Phone Number (505)986-6216	
VI. NEW MEXICO CJIS AGENCY COORDINATOR		

Full Name and Title: Emeterio Chavez Admissions & Release Records Manager	
Email Address: epchavez@santafecountynm.gov	Phone Number: (505)428-3843
VII. NEW MEXICO DPS AGENCY HEAD	
Full Name and Title: Jason Bowie - Secretary	
Email Address: N/A	Phone Number: N/A

SECTION 8: NEW MEXICO DIVISION OF CRIMINAL IDENTIFICATION CRIMINAL JUSTICE AGENCY USER AGREEMENT FOR CJIS SYSTEMS ACCESS ACKNOWLEDGMENT

As an Agency accessing CJIS systems and CJI within the state of New Mexico, we hereby acknowledge the responsibilities as set out in this document as well as those documentations incorporated by reference. The Agency also agrees to comply with all state and federal statutes and regulations as applicable and to use the information received from CJIS Systems only for purposes specifically authorized by New Mexico law. We acknowledge these responsibilities have been developed and approved by the NM DPS and/or the FBI in order to ensure the security, reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of CJIS systems.

This Agreement commences on the date the last signature is obtained below and continues until termination by either party. We acknowledge a failure to comply with these responsibilities will subject the NM DPS and this Agency to various sanctions as recommended by the (Directors) of the NM DPS and/or the FBI. The NM DPS reserves the right to suspend service to the Agency or an individual user when the security or dissemination requirements are violated to preserve the integrity of CJI data. This Agreement may be terminated sooner by one or both parties upon thirty (30)-day written notice or immediately upon violation of the Agreement. Compliance with this Agreement is voluntary; however, failure to complete this Agreement may result in denial of request.

In witness whereof, the parties hereto caused this agreement to be executed by the proper officers and officials.

Signature of Agency Head	Title and Printed Name	Date
	Gregory S. Shaffer Santa Fe County Manager	3/18/2026

Approved as to form by R.D.J., ACA, for
H.D. Santa Fe County Attorney 3/4/2026

Signature of TAC	Title and Printed Name	Date
	Emeterio Chavez	3/5/26
Signature of Assistant TAC	Title and Printed Name	Date
	ArmandoTrujillo	3/5/2026
	Dominic LeDoux	3/16/2026

Signature of OSPR	Title and Printed Name	Date
	Jason R. Boaz	4/1/26
Signature of DPS Secretary	Title and Printed Name	Date
	Administrative Records Manager	3/5/26
Signature of NM CJIS Agency Coordinator	Title and Printed Name	Date
Jessica A Mascareñas	CSO Jessica A Mascareñas	3-30-26
Signature of NM CSO or Designee	Title and Printed Name	Date

~~Date~~