NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor
Manny Barreras
Cabinet Secretary & State CIO

State of New Mexico: Data Policy Version 1.0 (3/2026)

PURPOSE:

The purpose of this Data Policy is to establish common guidelines for data quality, privacy, classification, and retention management across State of New Mexico agencies. A critical factor for effective government operations is the ability to share information and collaborate effectively and efficiently while satisfying the security and privacy requirements for protecting sensitive information. Conventional network-centric security measures are increasingly ineffective for protecting information as systems become more dispersed, mobile, dynamic, and shared across different environments and subject to different types of stewardship. Data classification practices enable data governance processes at scale. Through effective and responsible management of data, state agencies can promote trust, improve operational efficiency, and enable better service to the residents of New Mexico with accurate, transparent, and timely information, while protecting privacy and security, managing risk, and promoting accountability and equity.

Each Agency should implement its own data policy which, at a minimum, incorporates the standards and principles outlined in this Policy.

SCOPE:

This Policy applies to employees, contractors, and agents of New Mexico Executive Branch Agencies who create, edit, or manage data on behalf of an agency.

DEFINITIONS:

Agency: As defined in Section 9-27-3(A) NMSA 1978.

Data Governance Council: A council that provides ongoing oversight, ensuring alignment with organizational objectives and legal requirements.

Data Steward: An appointed or designated agency official with statutory or operational authority for specific information and responsibility for establishing controls for data generation, collection, dissemination, and disposal.

De-identification: De-identification refers to any process of removing the association between a set of identifying data and the data subject.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Pseudonymization: Pseudonymization refers to a de-identification technique that replaces an identifier (or identifiers) for an individual with a pseudonym in order to hide the identity of that individual.

Should/Shall: “Should” indicates that the Agency is expected to make a good-faith effort to achieve the stated

outcome when feasible, while “shall” denotes a mandatory requirement with which the Agency must comply.

PRINCIPLES:

- **Valid and Reliable**: Agencies must ensure that the data it produces is accurate, valid and reliable.
- **Privacy and Protection**: Agencies must ensure that in collecting and generating data, it adheres to privacy regulations and standards, including any applicable federal standards, and its practices respect privacy and ensure data protection.
- **Transparent and Auditable**: Agencies shall be as transparent as possible concerning the sources that have contributed to or influenced their data sets.

GUIDELINES:

Data Validation

Data values shall, to the greatest extent possible, be correct, complete, truthful, consistent, timely, deduplicated, and free from errors. Data shall represent the real-world scenario or event it is supposed to depict.

Privacy Practices

Agencies shall collect and process only the data needed for specific purposes, with no extraneous PII being collected or stored. Agencies should obtain consent and provide notice before using or disclosing PII data, and provide clear and concise information about data usage, repurposing, sharing, and options (if any) for withdrawing consent.

Data Protection

Agencies should aim to implement comprehensive safeguards to protect PII data from unauthorized access, disclosure, alteration, or destruction. These safeguards must include, at a minimum:

- ***Security Best Practices**: Apply strong access controls, encryption, and secure maintenance practices for all sensitive data.*
- ***Advanced Disclosure Avoidance**: In addition to removing direct identifiers in published data, agencies shall employ statistical and technical methods to reduce re-identification risks. Examples include:*
  - ***Primary and Secondary Value Suppression**: Suppress sensitive values in published datasets to prevent inference of individual identities.*
  - ***Noise Injection and Perturbation**: Introduce controlled variations in data to protect confidentiality while preserving analytical utility.*
  - ***Aggregation and Generalization**: Group data into broader categories to minimize disclosure risks for individuals or special populations.*
- ***De-identification and Pseudonymization**: Continue using these techniques as foundational measures, supplemented by advanced methods above.*
- ***Compliance with Best Practices**: Agencies must document and regularly review disclosure avoidance strategies as part of their governance and audit processes.*

Access and Stewardship

Agencies should afford individuals the right to request access to their PII data, review it for accuracy and request corrections when necessary. Agencies shall segregate PII data from records disclosed to the public and establish access controls according to law. Agencies should identify data stewards for each data set to promote accountability. Stewards' responsibilities should include defining access control to ensure compliance, maintain quality of the data, and ensure data integrity and security. Data stewards are responsible for maintaining permission structures (e.g., Entra ID groups) that enforce access controls based on classification levels.

Data Audits

Agencies should accurately attribute the sources that have contributed or influenced to their data sets and maintain sufficient first-level data or metadata to reconstruct, if necessary, the methods by which agencies have arrived at data outputs. Regular governance reviews by the Data Governance Council are an integral part of the audit process and issue management.

Data Retention

Each agency is responsible for retaining its records based on retention and disposal schedules developed by the State Commission of Public Records. To prevent data loss, particularly for electronic data, regular data backup is recommended. Frequency is based on the type of data and the risk of losing data and shall be regulated by each agency. Backups should be retained until the next full backup is successfully completed.

Data Classification

Information must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. Classification levels shall directly inform access control mechanisms. Agencies must implement permission structures—such as group-based access using Entra ID or equivalent identity management systems—to ensure only authorized groups can access documents according to their classification. Both classification and permissioning are required for robust access control. Data collected should come from a trusted source to ensure integrity of the data being collected. Data classification is conducted at the file or document level, according to the sensitivity labels shown below. Classifying data at this level is essential for responsible data management. Information may have different classifications during its life cycle. Agencies are responsible for periodic reclassification based upon business impact, changing business priorities and/or new laws, regulations, and security standards.

Each agency is responsible for classifying its data into one of the **SoNM Data Classification Framework** levels as follows:

- **Level 1: Published**
  - Records that are not protected from disclosure and not subject to redaction if disclosed. L1 records are freely shared both internally and externally, and any public release can generally

be authorized by employees at lowest level of the organization.
    - *Examples*: Press releases, brochures, pamphlets, public access websites, and materials created for public consumption.
- **Level 2: Internal**
    - Records that are not legally protected from public disclosure but are subject to internal access restrictions to facilitate organizational management and/or objectives. Release of L2 records must generally be authorized by employees at the level of a manager or above but release typically would not require a legal review.
    - *Examples*: Business plans, pay records, accounting records, internal audit reports, non-privileged emails, names and addresses that are not protected from disclosures.
- **Level 3: Sensitive**
    - Records that contain a mix of legally protected and unprotected information. Release of L3 records must generally be authorized by entity legal after redaction of legally protected information and verification of record law compliance.
    - *Examples*: Personal identifier information (PII)), information exempt from public records disclosure, portions of personnel files, confidential portions of law enforcement records.
- **Level 4: Restricted**
    - Records that are wholly legally protected or designated as confidential by an authorized functionary within the organization. Release of L4 records is prohibited except pursuant to strict legal parameters and processes, and any release must generally be approved by entity legal and/or high-level personnel within the entity.
    - *Examples*: Attorney/client communications, medical records, tax records.

An agency may establish additional classification levels based on the type of data it is responsible for managing. If an agency has established additional classification levels, it shall implement classification standards applicable to those levels that are consistent with this policy.

AGENCY-SPECIFIC POLICIES AND FEDERAL REQUIREMENTS

For any elements not explicitly defined within this Policy, agencies shall refer to their own internal data policies to ensure comprehensive coverage of operational, compliance, and governance needs. Each agency is responsible for maintaining a local data policy that aligns with this statewide framework while addressing unique requirements, including those mandated by federal regulations, funding agreements, or program-specific guidelines. Where federal requirements apply, agencies must incorporate those provisions into their policies and ensure consistency with applicable laws and standards.

IT GOVERNANCE AND COMPLIANCE:

Effective IT governance and compliance are crucial for the successful management of data within the New Mexico state government. This involves establishing clear policies, procedures, and controls to ensure that data management and use align with state objectives, regulatory requirements, and industry best practices.

- **Governance Framework**: An agency should implement a comprehensive governance framework to oversee data collection, usage, and disclosure. This may include defining roles and responsibilities, setting strategic goals, and establishing governance committees to monitor progress and address issues. **Oversight of data management policies and practices should be vested in the Data**

Governance Council, which should include the agency CIO, CISO, top-level agency leadership, and representatives from the Office of General Counsel (OGC), as applicable. The Council is responsible for policy approval, strategic direction, and resolution of escalated issues.

- **Policy Development**: An agency should develop and enforce policies that guide the ethical use, collection, and management of data systems; and ensure policies comply with these guidelines and applicable laws and regulations, including privacy and security.
- **Risk Management**: An agency should establish robust risk management practices to identify, assess, and mitigate potential risks associated with data collection systems. This involves continuous monitoring, regular audits, and timely updates to risk mitigation plans. In the case of any data breach, an agency shall notify the New Mexico Office of Cybersecurity and any applicable federal authority.
- **Compliance Monitoring**: An agency should regularly review data collection systems and processes for compliance with established policies, standards, and legal requirements; and conduct internal and external audits to ensure adherence to compliance obligations and readiness for potential regulatory inspections. The Data Governance Council should convene on a regular schedule (e.g., quarterly) to review data management issues, policy compliance, and audit findings. The Council should document issues, assign responsibility for resolution, and track progress to closure. This process ensures continuous improvement and audit readiness.
- **Training and Awareness**: An agency should provide ongoing training and awareness for state personnel involved in data collection systems. This ensures that all stakeholders understand their roles, responsibilities, and the importance of adhering to governance and compliance standards.
- **Security Review**: An agency should not purposely collect non-public information unless it has successfully completed a security review, and it has implemented and applied sensitivity labels and data classification to their data.

LINKS:

State Record Center and Archives Functional Record Retention and Disposition Schedules: Title 1 – General Government Administration NM Admin Code - State Records Center & Archives

State of New Mexico: Generative AI Use Guidelines Policy: Generative_AI_Use_Guidelines_Policy Signed.pdf

APPROVALS:

Version Date	Version Approved By	Version Comments
1.0 – March 2026	Manny Barreras DoIT Cabinet Secretary Signed by: Manny Barreras 32A0D0595C7C493... 3/10/2026	