NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor

Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Data Classification Policy**
Policy Number:	**DoIT-361-704**
Effective Date:	6/27/2022
Issued By:	**DoIT CIO**
Distribution:	**DoIT IT Resource Users**
Approved by:	**Raja Sambandam, Acting Cabinet Secretary**

1. AUTHORITY

Pursuant to the New Mexico Department of Information Technology Act, NMSA 1978, § 9-27-1 *et seq.*, the Secretary of the Department of Information Technology (DoIT or Department) shall exercise general authority over all department employees, manage all operations of the Department, and administer and enforce laws of which the Secretary or Department is charged.

2. PURPOSE

This Policy presents DoIT's data classification system for critical internal and customer data. Data classification is the foundation for specification of policies, procedures, and controls necessary to protect sensitive or confidential data. Data must be protected in a manner commensurate with its sensitivity and criticality, and in accordance with regulatory requirements, where applicable.

3. SCOPE

This Policy applies to all DoIT Information Technology (IT) Resource Users and all DoIT Information Systems.

4. DEFINITIONS

a. **DoIT IT Resource Users** - All DoIT employees, contractors, and any other users of DoIT IT resources.
b. **Confidential Data** – Confidential data, if compromised in some form or fashion, is likely to result in significant and/or long-term harm to the institution and/or individuals who own the data. It includes, but is not limited to, data that is marked as confidential, data a reasonable person would know is confidential, and data designated as confidential under State or federal laws or regulations.
c. **Data Classification –** A method of defining and categorizing data to determine type,protection requirements, access level, and labeling.
d. **Federal Taxpayer Information (FTI)** – Information used by the Internal Revenue Service to identify taxpayers' personal and business tax return data.
e. **Sensitive Data** – Sensitive data, when released without authorization, could be expected to cause minor or short-term harm to the institution or individuals whose data is released, andis intended

only for limited dissemination. It includes, but is not limited to, data that is marked sensitive, data a reasonable person would know is sensitive, and data designated as sensitive under State or federal laws or regulations.

f. **Personal Identifiable Information (PII)**– Information that can be used on its own or with other information to identify, contact, or locate an individual or to identify an individual in context.

g. **Public Data** – Data that may be freely disclosed without restriction.

h. **Health Insurance Portability and Accountability Act (HIPAA)**- The Privacy Rule standards address the use and disclosure of individuals' health information by entities subject to the Privacy Rule.

5. POLICY

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. Data collected should come from a trusted source to ensure integrity of the data being collected. DoIT data shall be classified into one of the following three categories:

a. **Confidential Data**

Examples of confidential data include, but are not limited to:

i. Individual financial and account data, such as:

1. Cardholder data, including Primary Account Number (PAN), cardholder name,expiration date, and service code;
2. Credit card, charge card or debit card numbers;
3. Retirement account numbers;
4. Savings, checking or securities entitlement account numbers;
5. Taxpayer information – FTI

ii. PII (except as determined to be public record), such as:

1. Social Security Numbers;
2. Personnel and/or payroll records;
3. Driver's license or State ID card;
4. Name, address, telephone number, vehicle description, photograph, height, weight, gender, age, driving-related medical conditions and fingerprints.

iii. HIPAA, such as:

1. Medical information;
2. Medical record numbers;
3. Diagnoses;
4. Any unique identifying number or code.

Confidential data must be:

i. Protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure;

ii. To the extent not public under the Inspection of Public Records Act, protected by a confidentiality agreement before access is allowed by third parties; and
iii. Be destroyed in accordance with State record retention laws and regulations when no longerneeded.

b. Sensitive Data

Examples of sensitive data include, but are not limited to:

i. Operational business information or reports, such as internal billing, usability reports,or other internal documentation;
ii. DoIT procedures; and
iii. DoIT internal communications to employees.
iv. System security parameters, such as:

1. System security vulnerabilities;
2. Documented security information;
3. Network, applications and security systems information;
4. Information regarding current deployment, configuration, and/or operation ofsecurity products or controls.

v. Risk assessment and audit records, such as:

1. Infrastructure risk assessments;
2. Infrastructure audit records;
3. DoIT risk audit findings and reports.

Sensitive data must be:

i. Protected to prevent loss, theft, unauthorized access, and unauthorized disclosure;
ii. To the extent not public under the New Mexico Inspection of Public Records Act, protected by a confidentiality agreement before access is allowed by third parties; and
iii. Destroyed in accordance with State record retention laws and regulations when no longer needed.

c. Public

Examples of public information includes, but are not limited to:

i. Public-facing websites
ii. Job postings
iii. Marketing brochures or materials

5.1. DATA CLASSIFICATION LABELING

Data classification labeling is handled procedurally as delegated by the DoIT Chief InformationSecurity

Officer (CISO).

Data classification should also maintain an inventory of the applications that manage PII information and provide updates to the Chief Information Officer (CIO) at a defined frequency for all new or modified PII data.

5.2. DATA DESTRUCTION

Data that no longer has a business need and need not be retained pursuant to State record retention laws and regulations may be destroyed in the following manner:

a. "Hard Copy" materials must be destroyed by shredding or by another approved process that destroys the data beyond recognition or reconstruction.

b. Electronic storage media shall be sanitized appropriately by overwriting or degaussingprior to disposal.

The data destruction process should also:

a. Ensure the data to be destroyed follows the change control process in accordance with the DoIT *IT ChangeManagement Policy* for appropriate record keeping; and

b. Be tested periodically to confirm the data has beenappropriately destroyed according to this Policy.

5.3. REPORTING COMPROMISED CONFIDENTIAL INFORMATION

Any suspicion of compromised data leaking must be reported to DoIT's CISO or CIO designee as soon as possible. Should the suspected data include PII, HIPAA, or other regulated customer information, an incident response procedure must be documented in compliance with *DoIT's Computer Incident and Customer Data Breach Response Policy*.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT CISO is responsible for overseeing dataclassification and policy enforcement.

b. DoIT IT Resources Users

All DoIT IT Resources Users are responsible for understanding and adhering to the *Data Classification Policy* and for appropriately labeling and storing data as it is generated.

7. EXCEPTIONS

The DoIT CIO or CISO must approve in advance and in writing any exception to this Policy.

8. VIOLATIONS OF POLICY

Any DoIT IT Resource User found to have violated this policy may be subject to disciplinary action, up to

and including termination of employment.

9. REFERENCES

a. National Institute of Standards and Technology SP800-53 r4: DI-1, DI-2, DM-3, MP-6(1), MP-6(2), RA-2, SE-1

b. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 8.2.1

c. Payment Card Industry Data Security Standards DSS v3: 9.6.1

10. CHANGE HISTORY

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
09/30/2020	2		Revision Draft
2/26/2021	3	Raja S	Revised and routed for Union approval
06/29/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
10/13/2021	5	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:
437214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary

6/27/2022

Date