

### PURPOSE

This policy directs the Nevada Department of Transportation (NDOT) to develop a data classification scheme and a formal description (taxonomy) of data class types within the department. All NDOT data, regardless of repository, storage location, or format, will be evaluated for sensitivity and risk of access or disclosure to unauthorized parties and will be classified such that appropriate security controls can be applied to protect the data asset.

### POLICY

The Nevada Department of Transportation Data Classification Policy establishes a scheme (framework) for classifying data based on its level of sensitivity, value, and criticality to NDOT in accordance with state information security policies, standards, and applicable Nevada Revised Statutes. Classification of data aids in determining levels of security controls for the protection of data.

Data that is not classified is considered Level 1 – Public data unless its classification is determined by the business data steward as otherwise via the approved classification procedure and process. Inactive data that is not classified will remain unclassified as long as it is not accessed or used. Archived data that is not classified may be classified when accessed and re-used.

Failure to adhere to this Data Classification Policy may result in disciplinary action(s).

This policy should be reviewed at a minimum bi-annually.

## 1. DEFINITIONS

---

### 1.1 Data Classification Levels

**1.1.1** Level 1 – Public: Data should be classified as Level 1 – Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to NDOT or its stakeholders. Examples of data eligible for public access include press releases, Transportation Board Meeting transcripts, and travel data summary statistics. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data. Data that is classified as NDOT Level 1 would be stored in information systems categorized as Low.

**1.2** Level 2 – Sensitive: Data should be classified as Level 2 – Sensitive when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to NDOT or its stakeholders. Disclosure of sensitive data and information is typically governed by specific laws or regulations (e.g., PII (per NRS 603A), Criminal Justice Information (CJI), HIPAA, etc.) that determine and protect confidentiality or are defined as sensitive in state policy standards (i.e., S.3.02.01). Data that is classified as NDOT Level 2 would be stored in information systems categorized as Moderate.

- 1.2.1** Level 3 – Restricted: Data should be classified as Level 3 – Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a high or significant level of risk, direct harm, or endanger NDOT assets or its stakeholders. Examples of restricted data include data protected by federal or state privacy regulations (e.g., Emergency Response Plan, Vulnerability Assessments per NRS 239C) and data protected by confidentiality agreements. Data that is classified as NDOT Level 3 would be stored in information systems categorized as High, and if managed in a cloud-hosted system may require a higher level of secure storage, which may include FedRAMP-certified storage (44 U.S.C. 35; OMB Circular A-130).

### 1.3 Risk and Potential Impact Levels

- 1.3.1** Low: Unauthorized disclosure of information is expected to have **limited** adverse effects on operations, organizational assets, or individuals. Low risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.
- 1.3.2** Moderate: Unauthorized disclosure of information is expected to have a **serious** adverse effect on operations, organizational assets, or individuals. Moderate risk of financial loss, legal liability, public distrust, or harm if this data is disclosed.
- 1.3.3** High: Unauthorized disclosure of information is expected to have a **severe or catastrophic** adverse effect on operations, organizational assets, or individuals. High risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed.

### 1.4 Security Objectives

- 1.4.1** Confidentiality: Ensuring that only authorized people have the appropriate access privileges to sensitive or restricted department data and information. [based on 44 U.S.C., Sec. 3542]
- 1.4.2** Integrity: Ensuring that no unauthorized changes are, or have been, made to data or information by any individual or system access. [based on 44 U.S.C., Sec. 3542]
- 1.4.3** Availability: Ensuring role-based access to data and information is provided when needed, by authorized users, and in the manner needed. [based on 44 U.S.C., SEC. 3542]

### 1.5 Data

- 1.5.1** Data: Facts represented as text, numbers, graphics, images, sound, or video. Data is the raw material used to represent information, or from which information can be derived. [DAMA – International]
- 1.5.2** Classification: A way to categorize data assets by assigning unique logical tags, or classes, to a data asset and is based on the business context of the data (e.g., Driver's License Number, Social Security Number, Homeland Security Data).
- 1.5.3** Structured: Refers to data that is organized in a predefined manner, typically in rows and columns, making it easily searchable and analyzable. This type of data is often stored in databases or spreadsheets, where each data point has a specific meaning or value within a fixed schema. Examples of structured data include relational databases, tables in spreadsheets, and data stored in SQL databases. [NDOT Service Provider Master with T.O. Agreement]

#### 1.5.4 Unstructured:

- a) Any document, file, graphic, image, text, report, form, video, or sound recording that has not been tagged or otherwise structured into rows and columns. [DAMA – International]
- b) Unstructured data does not have a predefined data model or is not organized in a systematic way. It is typically text-heavy and can include multimedia content, making it more complex to process and analyze. *Department records are most often in the form of unstructured data.* Examples of unstructured data include emails, social media posts, videos, images, and documents in various formats. [NDOT Service Provider Master with T.O. Agreement, *modified*]

1.5.5 NDOT Data: Structured, unstructured, documents, and other records of information that are collected, maintained, and used by the covered NDOT entities, for the purpose of carrying out NDOT business, even if subject to contractual or statutory limitations. NDOT Data may be stored either electronically or by paper and may take other forms including, but not limited to, text, graphics, images, sound, or video. NDOT Data is essential data required to conduct operations within the NDOT. This includes any data elements that are created, received, maintained, or transmitted. [NDOT Data Governance Policy]

#### 1.5.6 Archive:

- a) **Noun** – NDOT Data preserved in a secondary, lower cost storage location, for infrequent historical reference. [DAMA – International, *modified*]
- b) **Verb** – To move stored NDOT Data to a secondary, less readily accessed location, at lower storage costs, for historical reference. [DAMA – International, *modified*]

### 1.6 Roles

1.6.1 Business Data Steward: The person(s) responsible for updating stored data and ensuring the quality and reliability of NDOT Data. They also are the authority with respect to the business' data access.

1.6.2 Data Custodian: The individual/team responsible for providing technical support for the databases and/or applications where the data is stored.

1.6.3 NDOT Users: NDOT employees, volunteers, interns, third-party vendors, and contractors that have access to NDOT Data.

## 2. BACKGROUND

---

2.1 The State of Nevada Information Security Program's policies relevant to data classification were developed following guidelines and standards from the National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), and the Center for Internet Security (CIS) Controls. The State's Information Security Program Policy provides the following directives to state agencies:

### 2.1.1 Chapter 3 – Security Administration Policies

- **Section 3.1.1 C:** *Establish a process to determine information sensitivity, based on best practices, state directives, legal and regulatory requirements, and identified security risks and*

*vulnerabilities, to determine the appropriate level of protection for the information and the operational environment of the agency.*

- **Section 3.2.1 C:** *State information/data must be classified and protected based on its importance to business activities and risks to any given state agency.*
- **Section 3.2.3 A:** *Classify and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.*

### 2.1.2 Chapter 6 – CIS Controls

- **Section 6.13 – Data Protection:**
  - a) **CIS 13.1:** *Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.*

*State agencies must maintain an accurate and up-to-date inventory of sensitive information assets, including agency-defined essential data, system documentation, operational and support procedures, information security plans, and contingency and continuity of operations plans.*

## 3. SCOPE

---

This policy applies to all NDOT employees, contractors, consultants, contingent workers, and other entities who use or interact with NDOT Data for department business. Specifically, this policy applies to those who are responsible for classifying any NDOT Data and protecting NDOT Data associated with Level 2 – Sensitive or Level 3 – Restricted data classifications. The data covered by this policy may reside in any repository (e.g., relational or NoSQL database, file shares, network drives, document stores, or web sites) and location (i.e., on-premises or cloud storage).

The steps in the NDOT Data Lifecycle include the creation, acquisition, or receipt of data; active use (i.e., storage and management); an inactive period for data beyond active use (i.e., retention period); and eventually, its disposition (i.e., archive or delete/destroy). (Figure 1.)

**Figure 1.** NDOT Data Lifecycle



## 4. RESPONSIBILITY

---

Individuals responsible for data access, security, and stewardship are within the scope of this policy and includes NDOT's Data Management Office (DMO), Information Security Office (ISO), Records Management Office (RMO), Attorneys General Office (AGO), all business areas (Business Data Stewards), and information system leads (Data

Custodians) per NDOT Data Classification RACI Matrix. Individuals shall ensure an appropriate classification framework is determined, applied, and maintained following the Data Classification Procedure (Section 5) and applicable NDOT policies, procedures, processes, and standards. NDOT Users have a responsibility to ensure that all NDOT Data, structured and unstructured, are managed appropriately per its inherent classification, as defined or applied.

The NDOT Data Governance Committee (DGC), as the governing authority for NDOT Data, shall act as this policy's owner, and, as such, will provide guidance and direction on policy review and change, when necessitated, and ensure consistent policy adherence across NDOT business units. The DGC may establish ad hoc work groups as needed for related tasks or activities not explicitly described in the procedures (Section 5) and will facilitate policy-related communications and role-based training to business units.

Notwithstanding data and/or record access provisions provided for in NRS 239 and NRS 239C, access by external parties to Level 2 – Sensitive or Level 3 – Restricted NDOT Data shall be governed by a contractual agreement (e.g., data sharing agreement, memoranda of understanding).

## 5. PROCEDURE

---

The procedure for classifying data, after establishing a data classification policy, includes the following functions or processes:

**5.1** Develop and document an NDOT Data sensitivity taxonomy that can be applied to any NDOT Data. The taxonomy will cover the variety of data across Levels 1, 2, and 3 and be flexible to add more sensitivity classes (labels) and sensitive data types as needed. This activity is a collaborative effort between the Data Management Office, Information Security Office, Records Management Office, and Business Data Stewards.

**5.2** Identify NDOT Data assets to be classified. The inventory of data assets is directed from the Data Management Office and accomplished with key input from Business Data Stewards.

**5.2.1** Discovery: NDOT's existing data assets are identified, inventoried, and assessed with the assistance of Business Data Stewards, and Data Custodians as needed. Data in any location (on-premises or cloud-hosted) and repository are included in discovery regardless of the data store (i.e., both relational and NoSQL databases, and Excel workbooks if used for business operations data).

**5.3** Assess the data assets and determine the appropriate data classifications for each. NDOT's Chief Data Officer (CDO), or delegate(s), and Business Data Stewards evaluate data within each data asset for associated federal or state statute or other conditions that may affect a data's sensitivity to disclosure for determining the appropriate sensitivity class label and data type. **Note**: a data asset may have more than one sensitive data type, and thus, the most sensitive defines the classification for that data and IT system/application. Additionally, combined individual data elements that are L1 individually but in combination can elevate to L2 (i.e., personal information elements in growing combinations becomes L2 PII).

**5.3.1** Business Data Stewards evaluate security objectives for their data by rating the potential impact of compromise to data confidentiality, integrity, and accessibility on the department's business function/interest or individuals should there be a breach of security. Data stewards shall apply a Low, Moderate, or High impact level for each category per Section 1.2. The following tables will

be populated with sensitivity data classes and data types per data classification taxonomy and data inventory:

**Level 1 – Public Data**

Sensitivity Class and sensitive data types	Confidentiality	Integrity	Availability

**Level 2 – Sensitive Data**

Sensitivity Class and sensitive data types	Confidentiality	Integrity	Availability

**Level 3 – Restricted Data**

Sensitivity Class and sensitive data types	Confidentiality	Integrity	Availability

**5.4** Import data asset(s) into NDOT’s data governance application and scan the data for patterns and key words associated with NDOT’s classification taxonomy.

**5.4.1** Configure the data governance application to accommodate data classifications and sensitivity data types for the data asset(s) to be connected to the application. Verify that the appropriate pre-loaded system classifications are enabled/disabled, and that any custom classifications required are added and configured.

**5.4.2** Data custodians connect data assets to NDOT’s data governance application and perform data asset scans. Business Data Steward(s) for the data asset confirm/QC classification and sensitivity labels applied to tables, columns, or unstructured data.

**5.5** Associate data classification security level with the IT system where the data asset is stored. NDOT IT staff assign the classification sensitivity labels and ensure applicable controls are configured and applied so that security objectives and privacy requirements can be enforced within the system/application for each data asset.

**5.6** Monitor data assets for changes that may require updating data classifications and/or the data classification taxonomy. NDOT’s Business Data Stewards are responsible for monitoring their data assets for changes affecting classification, in consultation with NDOT’s CDO, or delegate. IT controls are monitored and assessed for validity on an annual basis.

## 6. REFERENCES

### 6.1 Related and Supporting Policies and Standards

Policy, Standard, Statue, or Document	Owner	Version
State Information Security Program <a href="#">Policy</a>	State CISO & CIO	H
Nevada Information Security Standard <a href="#">S.3.02.01 - Data Sensitivity</a>	State CISO & CIO	G
Nevada Information Security Standard <a href="#">S.3.04.01 - Personnel Security</a>	State CISO & CIO	J
Nevada Information Security Standard <a href="#">S.3.07.01 - Information Security Risk Analysis</a>	State CISO & CIO	D
Nevada Information Security Standard <a href="#">S.5.04.04 Data Security Architecture</a>	State CISO & CIO	C
Nevada Information Security Standard <a href="#">S.5.06.01 Cloud Services</a>	State CISO & CIO	G
Nevada Information Security Standard <a href="#">S.6.13.01 Data Protection</a>	State CISO & CIO	A
Nevada Revised Statutes: Chapter 239 – PUBLIC RECORDS ( <a href="#">NRS-239</a> )	Nevada Legislature	
Nevada Revised Statutes: Chapter 239C – HOMELAND SECURITY ( <a href="#">NRS-239C</a> )	Nevada Legislature	
Nevada Revised Statutes: Chapter 603A – SECURITY AND PRIVACY OF PERSONAL INFORMATION ( <a href="#">NRS-603A</a> )	Nevada Legislature	
Nevada Revised Statutes: Chapter 603A, Section 210 – SECURITY MEASURES ( <a href="#">NRS-603A.210</a> )	Nevada Legislature	A 2019, 2574
44 USC Chapter 35, Subchapter II: INFORMATION SECURITY ( <a href="#">44 U.S.C., SEC. 3542(b)(1)(A), (B), (C)</a> )	United States Congress	

APPROVED BY	SIGNATURE	APPROVAL DATE
NDOT ITC	RECORDED ON: <b>ITC PROPOSAL 85345</b>	05 FEBRUARY 2025

**ROUTING HISTORY** (This portion will be used to track the review, edit, and comment routing progress of the TP and will be deleted when finalized.)

Date	Change	Name / Division
<b>August 6, 2024</b>	<b>v 0.1</b> – Initial Submission	Michael Pipp / DMO
<b>August 27, 2024</b>	<b>v 0.2</b> – responses to comments; added sections 1.3, 1.4, and footer to Table 1.	Michael Pipp / DMO
<b>September 20, 2024</b>	<b>v 0.3</b> – Combined Heather’s comments; Provided this version to Microsoft.	Yesh Purkar / DMO
<b>October 2, 2024</b>	<b>v 0.4</b> – Copied Christian’s comments into document; added references to NRS 239 & NRS 239C to Section 6 table.	Michael Pipp / DMO
<b>October 30, 2024</b>	<b>v 0.5</b> – all sections reviewed by CFT. Comments resolved and edits made per collaborative discussion and consensus.	Michael Pipp / DMO
<b>November 14, 2024</b>	<b>v 0.6</b> – various grammatical edits made per CFT review and comments. Specifically, added a definition for Classification (Section 1.4.3); procedure steps for importing and scanning data assets into a data governance application (Section 5.4); and modified the references table to include NRS 603A and modified the Data Governance Policy RACI Matrix to the Data Classification RACI Matrix (Section 6.1).	Michael Pipp / DMO
<b>November 25, 2024</b>	<b>v 0.7</b> – various grammatical edits made per CFT review and comments. Section 3 Scope – deleted first sentence of ¶2 and moved remaining text, with some edits, to Policy section page 1, ¶2.	Michael Pipp / DMO
<b>January 16, 2025</b>	<b>v 0.8</b> – following IT Management review, edits made to POLICY statement clarifying data stewards are responsible for applying classification; revised definitions in Section 1.3; and an addition to the Note in Section 5.3.	Michael Pipp / DMO
<b>February 5, 2025</b>	<b>v 1.0</b> – Policy approved by ITC with the following revisions: revised the Business Data Steward definition to include “authority on data access,” added reference to Nevada Information Security Standard S.3.04.01 - Personnel Security to Section 6, and edited Section 6 for consistent presentation.	Michael Pipp / DMO