Joe Lombardo
Governor

Timothy D. Galluzi
Executive Director / State CIO

Darla J. Dodge
Senior Deputy Director / COO

Adam Miller
Deputy Director / OISCD

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | www.it.nv.gov | CIO@it.nv.gov | Fax: (775) 687-9097

1.0 PURPOSE

To establish a uniform, enterprise-wide framework for the classification of information assets across Nevada Executive Branch agencies. This policy provides a standardized four-tier data classification structure that enables consistent, risk-appropriate handling, protection, and lifecycle management of state data while preserving agency autonomy in classification decisions.

Data classification serves as the foundational layer enabling all downstream governance activities, providing a common language for cross-agency collaboration, data sharing agreements, retention schedules, and the application of appropriate technical controls.

Public Records Statement: Nothing in this policy changes the public's right to access government records under the Nevada Public Records Act (NRS Chapter 239). Classification tiers reflect internal handling requirements only.

This policy does not create, expand, or modify any exemption from disclosure under NRS Chapter 239 or other applicable law, and it does not authorize any Executive Branch entity to declare a record confidential absent a legal basis. Classification tiers are for **internal safeguarding and handling** and are not, by themselves, a legal basis to withhold a record or portion of a record.

2.0 SCOPE

This policy applies to:

- All Executive Branch agencies, departments, divisions, boards, and commissions
- All information assets created, collected, processed, stored, transmitted, or disposed of by or on behalf of the State of Nevada
- All state employees, contractors, vendors, and third parties who access, handle, or manage state information assets
- All information systems, applications, and platforms that store or process state data, regardless of hosting location (on-premises, cloud, or hybrid environments)

3.0 REFERENCES & RELATED POLICIES

State References

- NRS 242.101 – Duties of the Chief Information Officer
- NRS 242.105 – Confidentiality of certain information relating to security of information systems
- NRS 239 – Public Records
- NRS 603A – Security of Personal Information
- State Administrative Manual (SAM) Chapter 1600 – Information Technology
- State Information Security Program Policy, 100
- S.3.02.01 – Data Sensitivity Standard

Federal References

- NIST Special Publication 800-53 – Security and Privacy Controls
- NIST Special Publication 800-60 – Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST Cybersecurity Framework (CSF)
- CIS Controls v8

Regulatory Frameworks

- Health Insurance Portability and Accountability Act (HIPAA)
- Criminal Justice Information Services (CJIS) Security Policy
- IRS Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies (for Federal Tax Information)
- Payment Card Industry Data Security Standard (PCI DSS)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Processing Standards (FIPS)
- Controlled Unclassified Information (CUI) Program
- Confidential Information Protection and Statistical Efficiency Act (CIPSEA)
- General Education Provisions Act (GEPA)
- 20 CFR 603 - Confidentiality and Disclosure of State UC Information
- Privacy Act of 1974

4.0 DEFINITIONS

Classification Tier: One of four standardized levels (Public, Sensitive, Confidential, Restricted) assigned to information assets based on sensitivity, regulatory requirements, and potential impact of unauthorized disclosure.

Confidentiality: The property that information is not disclosed to unauthorized individuals, entities, or processes.

Data Owner: The individual or organizational unit with statutory or operational authority over specific data and accountability for its classification, protection, and appropriate use.

Data Steward: The individual designated by agency leadership to operationally manage data classification, handling, and protection activities within an agency.

Federal Tax Information (FTI): Federal tax returns and return information received from the Internal Revenue Service (IRS), protected under IRC 6103 and IRS Publication 1075.

Information Asset: Any data, information, document, record, or intellectual property that has value to the State, regardless of format (electronic, paper, or other media). This policy uses "information asset" rather than "data" to align with the NIST Risk Management Framework (SP 800-53) and CIS Controls terminology, which recognize that classification requirements apply not only to structured data (e.g., databases, spreadsheets) but also to unstructured content including documents, correspondence, images, system configurations, and paper records. While this policy is titled "Data Classification" for accessibility, the term "information asset" reflects the comprehensive scope of what must be classified and protected.

Integrity: The property that information has not been altered or destroyed in an unauthorized manner.

Need-to-Know: A determination that a prospective recipient requires access to specific information to perform official duties.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information.

Protected Health Information (PHI): Individually identifiable health information as defined under HIPAA.

Respondent Identifiable Information (RII): Information in an identifiable form which can be traced to an individual respondent to a protected survey. The term "identifiable form" means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means.

Regulated Data: Information subject to specific legal, regulatory, or contractual requirements governing its handling, storage, transmission, or disclosure.

5.0 POLICY

5.1 CLASSIFICATION FRAMEWORK

All information assets within the custody or control of Executive Branch agencies shall be classified according to the four-tier framework below. Examples are provided for illustrative purposes only and are not exhaustive. Agencies shall determine appropriate classification based on the definition and characteristics for each tier.

TIER 1: PUBLIC

Definition:

Information approved for unrestricted public disclosure with no harm potential if released.

Characteristics:

- No legal restrictions on disclosure
- Includes data which has already been made publicly available or data which may be made public without additional review or authorization.
- Unauthorized modification (not disclosure) may still require integrity controls

Examples:

- Press releases and public statements
- Published Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC)
- State agency annual reports and strategic plans published online
- Open data portal datasets (data.nv.gov)
- Public meeting agendas and approved minutes
- State budget documents released to the public
- Published job postings and employment opportunities
- Content approved for state agency websites and social media
- Data which has been accessed and retained from an outside publicly-available source.

TIER 2: SENSITIVE

Definition:

Internal information that is non-confidential but often privileged. While potentially sensitive or embarrassing if released, this information does not contain legally protected data. Information at this tier qualifies as a public book or record under NRS 239, and does not include information which is declared by law to be confidential, but requires review and approval prior to public release to ensure that it cannot be combined with other data to constitute PII, RII, PHI, or otherwise confidential data.

Characteristics:

- Not intended for proactive public distribution
- Subject to public records requests with appropriate review
- Requires review by a Data Owner, Data Steward, or other authorized individual before external release
- Access generally limited to need-to-know basis

Examples:

- Draft policies and administrative procedures under development
- Internal agency correspondence and memoranda

- Budget working documents and preliminary financial analyses
- Agency operational reports not intended for public distribution
- Non-confidential personnel information
- Internal meeting minutes
- State vendor information (non-confidential portions)
- Non-confidential policy position papers

TIER 3: CONFIDENTIAL

Definition:

Regulated data requiring significant protection due to legal, regulatory, or contractual obligations. Unauthorized disclosure could result in substantial harm to individuals, legal liability, or regulatory penalties.

Information in this tier may be contained within records that are subject to NRS Chapter 239; disclosure, redaction, or withholding decisions are made under applicable law and are not determined solely by this tier.

Characteristics:

- Subject to specific legal or regulatory protection requirements
- Unauthorized disclosure may result in penalties or legal action
- External sharing requires formal agreements
- Enhanced access controls and monitoring required

Examples:

- Personally Identifiable Information (PII): Social Security numbers, driver's license numbers, dates of birth combined with names
- Protected Health Information (PHI): Medical records, Medicaid eligibility data, health insurance information
- Respondent Identifiable Information (RII): Information about individual survey recipients or responses from federally-protected surveys or other surveys collected under a binding pledge of confidentiality.
- Payment Card Industry (PCI) data: Credit/debit card numbers, transaction data
- State criminal records not subject to federal CJIS requirements
- Child welfare case files and foster care records
- Employment security wage data and unemployment claims
- Mental health treatment records and substance abuse program data
- Attorney-client privileged communications and legal work product
- Educational records protected under FERPA Vocational Rehabilitation program records (Privacy Act, HIPAA)
- Unemployment Insurance information which identifies any individual or business entity (20 CFR 603)

- Individual program participant data under the Workforce Innovation and Opportunity Act (WIOA)

TIER 4: RESTRICTED

Definition:

Highest protection level for data subject to federal or state security requirements or critical to state operations. Unauthorized disclosure could cause severe harm to individuals, compromise law enforcement operations, threaten public safety, or violate federal security mandates.

Information in this tier may be contained within records that are subject to NRS Chapter 239; disclosure, redaction, or withholding decisions are made under applicable law and are not determined solely by this tier.

Characteristics:

- Subject to federal or state security mandates or critical operational requirements
- Unauthorized disclosure may cause severe or irreversible harm
- Access limited to personnel with specific authorization or clearances
- External sharing is prohibited except under specific legal authority

Examples:

- Criminal Justice Information Services (CJIS) data: FBI National Crime Information Center (NCIC) records, fingerprint data, federal criminal history
- Federal Tax Information (FTI): Tax returns and return information received from the IRS, protected under IRC 6103 and IRS Publication 1075
- Tax records and financial account information (state and federal)
- Controlled Unclassified Information (CUI): Federal data shared with state under specific handling requirements
- Critical infrastructure security data: Utilities control systems, emergency management tactical plans, vulnerability assessments
- Cybersecurity incident response data and active threat intelligence
- Encryption keys and cryptographic materials
- National security-related information shared with state agencies
- Active law enforcement investigative files involving federal cooperation
- Emergency operations center tactical response plans
- System credentials and administrative access credentials for critical state systems

The following principles shall guide all classification decisions:

A. Default to Higher Sensitivity: When uncertainty exists regarding the appropriate classification tier, information shall be classified at the higher (more restrictive) tier until a definitive determination can be made.

B. Classification Drives Governance: Data classification serves as the foundation for all downstream governance decisions, including but not limited to:

- Retention schedules
- Transmission and storage requirements
- Data sharing agreement terms
- Access control configurations
- Incident response procedures

C. Aggregate Data Consideration: Information that is individually classified at a lower tier may require reclassification to a higher tier when combined with other data if the combination increases sensitivity or enables identification of individuals. Similarly, protected individual data, when aggregated, may sufficiently protect the individual data it contains such that the product is less confidential than the source.

D. Highest Tier Prevails: When a dataset or system contains information spanning multiple classification tiers, the entire asset shall be protected according to the requirements of the highest classification tier present, unless technical controls enable effective segregation.

E. Lifecycle Classification: Classification determinations made by the Data Owner or source agency apply throughout the information lifecycle, from creation through disposition, both within and between agencies.

5.3 CLASSIFICATION RESPONSIBILITIES

A. State Data Governance Committee (SDGC)

The SDGC shall:

- Establish and maintain the four-tier classification framework as the standardized structure for Executive Branch agencies
- Advise and assist agencies in resolving questions about data classification or questions regarding framework interpretation
- Maintain a statewide registry of designated Data Owners and Data Stewards, as reported by agencies
- Review and recommend updates to this policy as needed

B. State Chief Information Officer (CIO)

The State CIO shall:

- Implement the framework through formal policy guidance
- Establish minimum requirements and baseline controls for each classification tier through complementary technical control policies developed in coordination with the Office of Information Security and Cyber Defense
- Oversee statewide compliance and report to the SDGC

C. State Chief Information Security Officer (CISO)

The State CISO, in coordination with the State Information Security Committee (SISC), shall:

- Develop and maintain technical control standards for each classification tier
- Provide guidance on security controls appropriate to each tier
- Support agencies in implementing classification-appropriate protections

D. Agency Heads

Agency heads shall:

- Ensure agency compliance with this policy
- Designate agency Data Owners and Data Stewards and report designations to the State Chief Data Officer
- Establish internal processes for classification review and approval
- Allocate appropriate resources for classification activities
- Coordinate classification implementation with the agency's public records function (records officer/coordinator) and assigned DAG so that public records responses remain compliant with NRS Chapter 239 and are not based on classification labels.

E. Agency Data Stewards

Agency Data Stewards shall:

- Serve as the primary decision-makers for classification within their organizations
- Coordinate with Data Owners to ensure appropriate classification determinations
- Maintain agency data inventories with classification assignments
- Escalate complex or high-stakes determinations to agency leadership
- Coordinate with appropriate staff, legal counsel, agency partners, etc., for classification guidance as needed.

F. Data Owners

Data Owners shall:

- Classify information assets within their authority according to this framework
- Document classification decisions with supporting rationale
- Establish a procedure to review classifications periodically or upon significant change
- Ensure appropriate handling and protection consistent with classification
- Coordinate with appropriate staff, legal counsel, agency partners, etc., to ensure appropriate classification of data.

G. All Personnel

All state employees, contractors, and authorized users shall:

- Handle information according to its assigned classification

- Report suspected misclassification or inappropriate handling
- Complete required training on data classification and handling

5.4 CLASSIFICATION PROCEDURES

A. Initial Classification

1. Data Owners shall classify information assets upon creation or acquisition
2. Classification decisions shall be documented and maintained in agency data inventories
3. Agencies are shall consult with their assigned Deputy Attorneys General (DAGs) when making classification determinations involving legal, regulatory, or statutory requirements

B. Classification Assignment Review

1. All classification assignments shall be reviewed according to an established schedule.
2. Reviews shall consider changes in:
    - Legal or regulatory requirements
    - Business needs and operational context
    - Associated risks
    - Aggregation with other data

C. Reclassification

1. Information may be reclassified when circumstances warrant
2. Reclassification decisions shall be documented with rationale
3. When information is reclassified to a higher tier, protection measures shall be implemented immediately
4. When information is reclassified to a lower tier, agencies shall verify that all regulatory and legal requirements for the new tier are met

D. Classification Labeling

1. Agencies shall establish procedures for labeling classified information appropriate to the medium and tier

E. Public Records Requests (NRS 239) – Separate Process

1. Processing, review, redaction, and production of records in response to a public records request shall be conducted under NRS Chapter 239 and applicable case law, in consultation with the agency's assigned Deputy Attorney General (DAG) as appropriate.
2. Classification labels or tier assignments shall not be used as the legal authority for denial or redaction in a public records response. Any denial or redaction must be supported by applicable law, including statutory authority and/or recognized legal privileges and balancing standards.

3. Agencies shall not implement search, collection, or production methods that automatically exclude responsive records solely because a classification tier is present.

5.5 AGENCY AUTONOMY

A. Classification Authority

Individual agencies retain full autonomy to determine how specific data assets originating within their agency are classified within the established four-tier framework. Data shared or provided by another agency shall be classified according to the original Data Owner's determination. Agency classification decisions shall reflect:

- Mission-specific requirements
- Applicable statutory obligations
- Regulatory mandates
- Operational considerations unique to each agency

B. Agency-Specific Requirements

Agencies may establish additional handling requirements for specific data types while maintaining the core four-tier structure. Such requirements must meet or exceed the minimum standards established for each tier.

C. Sub-Categories

The framework allows for specialized sub-categories within each tier to address specific regulatory requirements (e.g., HIPAA, CJIS, CUI, FTI, AI Training Data). Agencies establishing sub-categories shall:

- Document sub-category definitions and requirements
- Ensure sub-category controls meet or exceed tier minimum requirements
- Report sub-category usage to the SDGC upon request

5.6 TECHNICAL CONTROLS

Specific technical controls for each classification tier shall be established through complementary policies developed by the Office of Information Security and Cyber Defense in coordination with the SISC and relevant stakeholders. Until such policies are adopted, agencies shall implement controls appropriate to each tier based on:

- Existing state security standards (S.3.02.01 Data Sensitivity and related standards)
- NIST and CIS Control frameworks
- Applicable regulatory requirements

5.7 TRAINING

1. All personnel with access to state information shall complete data classification awareness training
2. Data Stewards and personnel with classification responsibilities shall complete enhanced training on classification procedures
3. Training shall be updated as this policy and complementary standards are revised

6.0 COMPLIANCE

6.1 Monitoring and Auditing

Agencies shall participate in periodic reviews of classification practices and compliance with this policy.

6.2 Non-Compliance

Failure to comply with this policy may result in:

- Remediation requirements
- Escalation to agency leadership
- Reporting to SDGC
- Other actions as determined appropriate

6.3 Incident Reporting

Suspected or confirmed incidents involving mishandling of classified data shall be reported in accordance with State Information Security Incident Management procedures.

7.0 EXCEPTIONS

Requests for exception to this policy must be:

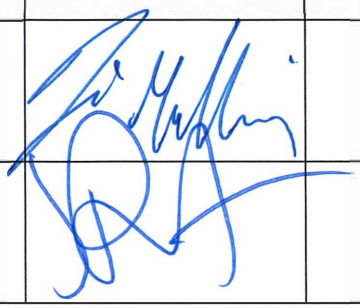
1. Documented in writing with business justification
2. Submitted to the State Data Governance Committee
3. Approved by the State Chief Information Officer

Exceptions shall be reviewed annually and shall not extend beyond two years without renewal.

8.0 POLICY MAINTENANCE

This policy shall be reviewed biennially by the State Data Governance Committee, or more frequently if warranted by changes in legal requirements, technology, or operational needs.

APPROVED BY

Title	Signature	Date
State Chief Information Officer		2/02/2026
State Chief Data Officer		2/02/2026

DOCUMENT HISTORY

Revision	Date	Change
A	2/02/2026	Initial release

APPENDIX A: GLOSSARY OF ACRONYMS

Acronym	Definition
BLS	Bureau of Labor Statistics
CIO	Chief Information Officer
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
CUI	Controlled Unclassified Information
DAG	Deputy Attorney General
DCFS	Division of Child and Family Services
DETR	Department of Employment, Training and Rehabilitation
FERPA	Family Educational Rights and Privacy Act

FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
GEPA	General Education Provisions Act
GTO	Governor's Technology Office
HIPAA	Health Insurance Portability and Accountability Act
IRC	Internal Revenue Code
IRS	Internal Revenue Service
ISO	Information Security Officer
NAC	Nevada Administrative Code
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
NRS	Nevada Revised Statutes
PCI	Payment Card Industry

PHI	Protected Health Information
PII	Personally Identifiable Information
RII	Respondent Identifiable Information
SAM	State Administrative Manual
SDGC	State Data Governance Committee
SISC	State Information Security Committee
STGC	State Technology Governance Committee
WIOA	Workforce Innovation and Opportunity Act

APPENDIX B: CLASSIFICATION QUICK REFERENCE

Tier	Name	Definition	Key Characteristics
1	PUBLIC	Information approved for unrestricted public disclosure	No disclosure restrictions; integrity controls may apply

2	SENSITIVE	Internal, non-confidential information requiring review before release	Need-to-know access; subject to public records with review
3	CONFIDENTIAL	Regulated data with legal protection requirements	Mandatory protections; formal agreements for sharing
4	RESTRICTED	Highest protection for federal or state security requirements or critical operations	Specific authorization required; sharing generally prohibited

APPENDIX C: RELATED COMPLEMENTARY POLICIES (PLANNED)

The following complementary policies establishing specific technical controls for each classification tier are planned for development:

1. **Technical Controls for Tier 1 (Public) Data** – Integrity controls, publication review processes
2. **Technical Controls for Tier 2 (Sensitive) Data** – Access controls, transmission standards, review procedures
3. **Technical Controls for Tier 3 (Confidential) Data** – Encryption requirements, MFA, logging, Data Sharing Agreement templates
4. **Technical Controls for Tier 4 (Restricted) Data** – FIPS encryption, secure enclaves, clearance requirements, federal compliance

These policies will be developed in coordination with the Office of Information Security and Cyber Defense, the State Information Security Committee (SISC), and relevant stakeholders.