FOR IMMEDIATE RELEASE
(Embargoed until February 11th at 8am (PST)

Nevada Establishes Statewide Framework to Modernize Data Privacy Ahead of 2026

CARSON CITY, Nev. — As state governments nationwide grapple with rising cyber threats and growing volumes of digital information, Nevada is taking a proactive step to modernize how public data is protected.

The State of Nevada has adopted the **Statewide Policy for Data Classifications (SDGC-2026-001)**, a uniform framework that establishes how information across the Executive Branch is identified, classified, and safeguarded based on risk and regulatory requirements. The policy takes effect in February 2026 and applies to all executive agencies.

Rather than relying on agency-specific practices or informal methods, the policy introduces a consistent, enterprise-wide approach designed to reduce risk, improve data sharing, and support future security 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.

By clearly defining default classifications and handling expectations, the policy is also expected to **enable more efficient data sharing across state agencies**. Agencies can now rely on a shared baseline for how information is categorized and protected, reducing uncertainty and hesitation when exchanging data. In many cases, this common framework may eliminate the need for separate, bespoke data-sharing agreements or significantly simplify them, allowing agencies to focus less on negotiating protections and more on delivering services and outcomes.

“This policy creates a common language for protecting information across state government,” said a spokesperson for the Governor’s Technology Office. “It ensures sensitive data is handled appropriately while still allowing agencies to share information and deliver services effectively.”

A Four-Tier Approach to Data Protection

At the core of the policy is a standardized four-tier classification system, organized by potential harm and legal obligations:

- **Public** — Information approved for unrestricted disclosure, such as public meeting agendas or published job postings.
- **Sensitive** — Internal, non-confidential information intended for operational use, including draft documents and internal communications.

- **Confidential** — Legally protected data where unauthorized disclosure could cause substantial harm, such as Social Security numbers, medical records, or financial information.
- **Restricted** — The highest protection level, covering information subject to federal security requirements or critical state operations, including criminal history records, cybersecurity defense plans, and encryption keys.

The policy requires that when classification is unclear, information must be treated at the higher protection level until a final determination is made.

Expanding What Counts as Protected Information

Unlike earlier approaches focused primarily on databases, the policy defines **"information assets"** broadly. It applies to data in any format, including paper records, emails, system configurations, images, and intellectual property.

This expansion reflects a shift in how governments view risk, recognizing that technical documentation and system designs can be as sensitive as the data they support.

Addressing Aggregated Data Risk

The policy also accounts for the "mosaic effect," where information that appears harmless in isolation can become sensitive when combined with other data. Agencies are required to reassess classification when aggregation increases the potential to identify individuals or expose protected patterns.

Clear Accountability and Governance

To support consistent implementation, the policy clarifies roles and responsibilities. **Agency Data Stewards** are designated as the primary decision-makers for classification within their organizations, while **Data Owners** retain authority and accountability for documenting classification decisions.

Mandatory training for state personnel will accompany rollout of the policy to ensure consistent understanding and application.

Laying the Groundwork for Future Security Controls

The data classification framework serves as the foundation for forthcoming technical safeguards, including multi-factor authentication, enhanced logging, and encryption standards aligned with federal requirements.

Together, these measures are intended to strengthen Nevada's overall digital resilience while enabling responsible data sharing across agencies.

An explainer video detailing the policy is available at:
https://youtu.be/fQmP2SxhZos

Media Contact:
Governor’s Technology Office
Email: Michaelhbm@it.nv.gov
Phone: 7754950603