Joe Lombardo
Governor

Timothy D. Galluzi
State Chief Information Officer

Darla J. Dodge
Deputy CIO – COO

David 'Ax' Axtell
Deputy CIO – CTO

Bob Dehnhardt
Deputy CIO - CISO

STATE OF NEVADA
GOVERNOR'S OFFICE
Office of the Chief Information Officer
100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | it.nv.gov | CIO@it.nv.gov | Fax: (775) 687-9097

Policy on the Responsible and Ethical Use of Artificial Intelligence in Nevada State Government Executive Branch

Purpose

The purpose of this policy is to ensure that the use of Artificial Intelligence (AI) within Nevada State Government's executive branch is conducted responsibly, ethically, and transparently. This policy establishes minimum standards for AI deployment and utilization, balancing safety and compliance with the flexibility needed for innovation across different agencies.

Definitions

- **Artificial Intelligence (AI):** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
- **Generative AI (GenAI):** AI algorithms and models that can create new content, including audio, code, images, text, and video, based on the data they are trained on.
- **Synthetic Media:** Media content, including but not limited to text, images, and videos, substantially generated or modified by AI technologies that mimic human-like outputs.
- **AI Transparency:** The requirement for clear documentation and disclosure of AI methodologies, data use, decision-making processes, and AI management protocols.
- **Digital Provenance:** Information detailing the origins, context, and authenticity of digital content, ensuring traceability and integrity.
- **Bad Actor:** An individual, group, or entity that intentionally uses artificial intelligence systems or synthetic media to commit fraud, spread misinformation, or perform any illegal activities under state or federal law.
- **Misuse of AI:** The application of artificial intelligence technology in a manner that is unethical, not transparent, or intended to harm individuals, manipulate public opinion, or disrupt legal and societal norms.

Principles

1. **Fairness and Equity:** AI systems must mitigate harmful biases to avoid discrimination or disparate impact based on race, color, ethnicity, sex, religion, age, disability, veteran status, marital status, sexual orientation, gender identity, genetic information, or any other classification protected by law.
2. **Innovation:** AI should be leveraged to improve state services and resident outcomes, used responsibly, and aligned with human-centered and mission-focused goals.
3. **Privacy:** AI implementations must preserve individuals' privacy rights by design, ensuring data handling aligns with all applicable laws and regulations.
4. **Safety and Security:** Adopt best practices and standards to identify and mitigate AI-related safety risks, ensuring resilience against threats.
5. **Validity and Reliability:** Maintain mechanisms to ensure AI systems work as intended, with accurate outputs and robust performance.
6. **Transparency, Accountability, and Explain-ability:** AI use should be well-documented and disclosed, enabling accountability and explain-ability to oversight bodies and residents, with clear human oversight.

Governance Structure

To ensure adherence to these principles, the following governance structure is established:

1. **State Technology Governance Committee (STGC):** Comprising representatives from various state departments and agencies, will assist with the help of The AI and Emerging Technology working group in developing and implementing AI policies, standards, and guidelines. This group will include experts in AI, data management, cybersecurity, legal, and ethics.
2. **The Office of the Chief Information Officer (OCIO)**will oversee the implementation and adherence to this AI policy. The STGC will collaborate with the AI Working Group to ensure comprehensive governance and management of AI technologies across Nevada's Executive Branch State Government.

Responsibilities

- Promote the principles set forth in this policy.
- Advise the Governor on AI-related matters.
- Facilitate statewide coordination on AI use.
- Develop baseline AI tool policies, processes, and standards, while supporting agencies in developing more stringent policies where needed.
- Leverage the expertise of the State Information Security Committee (SISC) to create a comprehensive AI risk and security policy, ensuring robust protection for AI systems and data.
- Ensure continuous monitoring and legal analysis of AI tools, with agencies conducting additional monitoring as required.
- Ensure human involvement in AI decision-making processes to maintain accountability and ethical oversight, allowing agencies to determine the appropriate level of oversight for their use cases.

Agency Flexibility

- **Agency-Specific Policies:** Each agency within the executive branch is encouraged to develop its own AI policy that meets or exceeds the baseline standards outlined in this document. Agencies should consider their specific use cases, risks, and ethical considerations when developing these policies.
- Agencies creating their own AI policies, should submit their policies to the STGC annually, prior to July 1, to the STGC Chair for committee review. The STGC may provide feedback or recommendations to the agency.
- In cases where Agency-specific policy and statewide policy may be in conflict, the more stringent policy shall have precedence. In all other cases, no Agency-level policy should be more lenient than statewide policy.
- **Enhanced Security and Risk Management:** Agencies are permitted and encouraged to implement additional security and risk management measures as deemed necessary to protect their unique operations and data, in collaboration with the SISC.

Acceptable Use

1. **Compliance with Baseline and Agency-Specific Policies:** Use of AI must comply with this baseline policy and any additional restrictions or guidelines established by the respective agency.
2. **Procedure for Questions and Reporting Violations:** If you have any questions regarding generative AI usage or would like to report policy violations, please contact the designated department/entity/team at the provided contact information.
3. **Examples of Use Cases** (this list is not meant to be exhaustive)**:**
   - **Permissible:** Brainstorming ideas, summarizing public data.
   - **Approval-Required**: Generating official reports, using AI-generated insights for policy decisions.
   - **Non-Permitted:** Creating discriminatory content, using personal data without anonymization.
   - Clarification of permissible versus non-permissible use cases shall be managed though the states traditional IT procurement governance process, the Technology Investment Notification (TIN).

Security and Compliance

- **Security Rules for Public and Proprietary GenAI:** Compliance with established security rules for data management and application development is required, with agencies able to impose stricter controls as needed, supported by the SISC.
- **Monitoring and Reporting:** Security teams must monitor and report potential security policy violations in AI use, with agencies encouraged to establish additional monitoring protocols.
- **Controlled Environments:** AI experimentation should only occur in secure, controlled environments, with agencies defining the specifics of these environments based on their risk assessments.

Accountability and Human Involvement

1. **Establishing Accountability:** Legal and compliance specialists should define and oversee AI accountability within the organization.

2. **Human Oversight:** Ensure critical AI decisions involve human review to maintain ethical standards.

Implementation Plan

1. **AI Action Plan:** Develop and implement a comprehensive plan that aligns with NIST's AI Risk Management Framework, including:
   - Establishing policies, processes, standards, and contracts for AI tools.
   - Embedding risk-based assessments into state processes.
   - Ensuring continuous monitoring and legal analyses of AI tools.
2. **Identify AI Use Cases:** Evaluate infrastructure to safely test AI proofs of concept and pilots, with a repeatable playbook for AI project management.
3. **Safety and Security Measures:** Implement safety prompt engineering to ensure AI interactions are confined within ethical and security boundaries. Establish mandatory safety training for all personnel involved in AI operations, with updates on policies and practices at least quarterly.
4. Agency Information Security Officers will be encouraged to include AI-related content in annual security awareness training for all state employees.

Data Handling Protocols

1. **Data Classification:** Classify data into categories such as aggregate, de-identified, and anonymous, with specific handling protocols for each to safeguard confidentiality and privacy.
2. **Data Protection Standards:** Require all AI systems to adhere to stringent data protection standards, including encryption and access controls.

Threat Identification and Mitigation

- **Regular Assessments:** Conduct regular security risk assessments, with agencies conducting additional assessments as needed, leveraging the SISC's expertise.
- **Mitigation Strategies:** Develop strategies to address identified risks, allowing agencies to implement additional strategies based on their specific risk profiles.

AI Misuse and Bad Actor Provisions

1. **Prohibitions and Penalties:** Existing law and state policy, as outlined in NRS 205.473 to NRS 205.513, stipulate that it is unlawful for any person or entity to use artificial intelligence or synthetic media to:
   - Engage in deceptive practices, including but not limited to the creation and dissemination of manipulated media or information designed to mislead the public.
   - Facilitate or conduct activities that infringe on privacy rights or data protection laws, as detailed in NRS 603A.
   - Manipulate or alter data to commit fraud, steal identities, or cause financial harm to individuals or entities, as covered under NRS 205.0832.
2. **Reporting and Response:** Establish a mandatory reporting system for suspected AI misuse, with agencies defining their own reporting processes and response teams.

Auditing

- **Compliance:** Agencies must report AI-related incidents and participate in regular audits, with the flexibility to conduct additional audits as needed.

- **Audit Reporting:** Document findings and develop action plans based on audit results, with agencies empowered to implement more frequent audits.

Continuous Improvement

- **Feedback Mechanisms:** Regularly review feedback from employees, stakeholders, and residents to inform policy updates, allowing agencies to establish their own feedback mechanisms.
- **Policy Updates:** The OCIO, in collaboration with the STGC, and AI and Emerging Technologies Working Group will review and update this policy annually, with agencies encouraged to update their own policies based on evolving needs.

Compliance

All state agencies must comply with this policy and related standards as a minimum requirement but are encouraged to develop more stringent policies and standards to address their specific needs.

References:

Nevada Revised Statutes (NRS) Chapter 242 - Information Services
NIST AI Risk Management Framework
Nevada Administrative Code (NAC) Chapter 333 - Purchasing: State
OCIO Agency Update Document

Timothy Galluzi, State Chief Information Officer
Office of the Governor, Office of the CIO
Chair, State Technology Governance Committee

Effective Date: November 26, 2024