STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER: **400.014**
EFFECTIVE DATE: **12/16/2025**
REVISED:

AUTHORITY: **BOCC**
COUNTY MANAGER: **AO**

SUBJECT: RESPONSIBLE AND ETHICAL USE OF ARTIFICIAL INTELLIGENCE

I. Purpose:

This policy is designed to ensure that the use of Artificial Intelligence (AI) within Storey County is conducted in a responsible, ethical, and transparent manner. It emphasizes clear, accurate, and accessible communication while promoting the thoughtful integration of AI technologies. AI may be leveraged to enhance operational efficiency, support informed decision-making, and foster innovation. This policy sets forth minimum standards for the deployment and use of AI, striking a balance between safety, regulatory compliance, and the flexibility required to encourage innovation across all departments.

II. Definitions:

1. **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 utilize both machine- and human-based inputs to perceive real and virtual environments, abstracting such perceptions into models through automated analysis; and employ model inference to formulate options for information or action.
2. **AI Tools:** Any software, platform or technology that employs machine learning, natural language processing, robotics, or other AI capabilities to support balance operations.
3. **AI Transparency:** The requirement for clear documentation and disclosure of AI methodologies, data use, decision-making processes, and AI management protocols.
4. **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.
5. **Deepfake Technology:** Uses artificial intelligence (AI) to manipulate audio or video to create a false but realistic video of individuals doing or saying things they did not actually do or say.
6. **Digital Provenance:** Information detailing the origins, context, and authenticity of digital content, ensuring traceability and integrity.
7. **Ethical AI:** Involves the responsible development, deployment, and utilization of Artificial Intelligence (AI) systems in a manner that promotes fairness, accountability, transparency, privacy, and respect for human dignity with a beneficial impact to address relevant problems and improve quality of life.

8. **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.
9. **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.
10. **Open-Source AI:** Software available for free to use, study, modify, and share.
11. **Proprietary IA:** Artificial intelligence (AI) that is developed and controlled by a single company.
12. **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.
13. **Unethical AI:** Applications that include deceptive practices, perpetuate biases and discrimination, infringe upon privacy rights and human rights, or cause unintended harm.
    a) Examples of unintended harm:
        I. Bias and discrimination, such as hiring algorithms.
        II. Privacy violations, such as data breaches.
        III. Errors and failures such as inaccurate or fabricated information.
        IV. Socioeconomic impacts, such as job displacement.
        V. Security risks and malicious use, such as cybersecurity threats.
14. **Voice Synthesis:** AI-generated speech that can mimic human speech.
15. **Text Generation:** AI-written text.
16. **Image Synthesis:** AI-generated images.

III. Principles:

1. **Compliance:** All AI tools must comply with applicable laws, industry regulations, and internal accounting policies regarding data protection, discrimination and fairness.
2. **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.
3. **Innovation:** AI shall be leveraged to improve county services and resident outcomes, used responsibly, and aligned with human-centered and mission-focused goals.
4. **Privacy:** AI implementations must preserve individuals' privacy rights by design, ensuring data handling aligns with all applicable laws and regulations.
5. **Safety and Security:** Systems must be developed and used with high standards of cybersecurity to protect against data breaches, manipulation or unintended access to sensitive information. All work must be scanned prior to implementation.

6. **Validity and Reliability:** Maintain mechanisms to ensure AI systems work as intended, with accurate outputs and robust performance.
7. **Transparency, Accountability, and Explainability:** AI use shall be well documented and disclosed, enabling accountability and explainability to oversight bodies and residents, with clear human oversight.

IV. Governance Structure:

1. To ensure adherence to these principles, the following governance structure is established:
   a) Representatives from various county departments will assist in developing and implementing AI policies, standards, and guides.
   b) The Storey County Human Resources office will oversee the implementation and adherence to this AI policy and will collaborate with departments to ensure comprehensive governance and management of AI technologies across Storey County**.**

V. The Storey County District Attorney's office will ensure that the AI policy is compliant with all relevant laws and regulations, as well as provide guidance and advice on its implementation and enforcement.

1. **Responsibilities:**
   a) Promote the principles set forth in this policy.
   b) Advise the County Manager and the Storey County Board of Commissioners on AI-related matters.
   c) Facilitate county coordination on AI use.
   d) Develop baseline AI tool policies, processes, and standards, while supporting departments in developing more stringent policies where needed.
   e) Create a comprehensive AI risk and security policy, ensuring robust protection for AI systems and data.
   f) Ensure continuous monitoring and legal analysis of AI tools, with departments conducting additional monitoring as required.
   g) Ensure human involvement in AI decision-making processes to maintain accountability and ethical oversight, allowing departments to determine the appropriate level of oversight for their use cases.
   h) Employees may only use AI tools that have been approved by the county IT Department. Unauthorized AI applications or systems shall not be used to handle county data or processes without prior approval by IT and or the county manager.
   i) Employees must ensure that AI tools are used in compliance with the county's data privacy policies, including obtaining necessary consents and ensuring secure data handling.
   j) Employees must receive training in the proper use of AI tools to ensure they understand their capabilities, limitations, and any ethical considerations.

k) Employees are responsible for the outcomes of tasks that use AI, ensuring human oversight in key decision-making processes. Employees must disclose if AI was used to produce or enhance, and not limited to, procedures, processes, code, scripts, and the like.

VI. Department Flexibility:

1. Department-Specific Policies: Each department within Storey County is encouraged to develop its own AI policy that meets or exceeds the baseline standards outlined in this document. Departments should consider their specific use cases, risks, and ethical considerations when developing these policies.
2. In cases where Department-specific policy and countywide policy may be in conflict, the more stringent policy shall have precedence. In all other cases, no Department-level policy shall be more lenient than countywide policy.
3. **Enhanced Security and Risk Management:** Departments 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 IT.

VII. Acceptable Use:

1. AI may be used to streamline repetitive tasks, improve workflows, and enhance public service efficiency.
2. Employees may use AI-powered tools for document processing, scheduling, drafting reports, emails, or communications, and basic administrative functions.
3. AI may be utilized for data analytics to support evidence-based decision-making. These tools are meant to augment human decision-making, not replace it. Employees may use AI to assist in evaluating information but must maintain accountability for final decisions.
4. AI-driven insights must be verified by human oversight to ensure accuracy, fairness, and compliance with county administrative policies.
5. Employees will monitor AI systems for biases, to ensure that AI-generated outputs are free from unfair biases, especially in recruitment, performance evaluation, and customer interactions.
6. AI-generated responses may be used to assist with public inquiries and for public communications, but responses must be fact-checked before release.
7. Synthetic media may be utilized for non-deceptive news and other content, creating realistic images and videos.
8. Compliance with Baseline and Department-Specific Policies: Use of AI must comply with this baseline policy and any additional restrictions or guidelines established by the respective Department.
9. 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 Human Resources Department.

10. AI can be used to automate repetitive tasks to increase efficiency. However, employees must monitor these automated processes to avoid errors and ensure quality control.

VIII. Prohibited Use

1. Prohibitions and Penalties: Existing law and state policy, as outlined is in conformance with NRS 205.473 to NRS 205.513 no county employee is permitted to use artificial intelligence or synthetic media to:
   a) Engage in deceptive practices, including but not limited to the creation and dissemination of manipulated media or information designed to mislead the public.
   b) Facilitate or conduct activities that infringe on privacy rights or data protection laws, as detailed in NRS 603A.
   c) Manipulate or alter data to commit fraud, steal identities, or cause financial harm to individuals or entities, as covered under NRS 205.0832.
2. AI shall not be used to make final decisions without human review.
3. AI must not be used to process or analyze sensitive, classified, or personally identifiable information (PII) unless specifically approved by the County Manager and reviewed by the District Attorney's Office, and determined to be secured in accordance with county internet and security policies
4. AI applications must not be used to cause discrimination, bias, or unfair treatment based on race, gender, age, disability, or any other protected class.
5. Employees may only use AI tools that have been approved by the IT Department and County Manager, and which comply with county security protocols and administrative policies.

IX. AI Misuse and Bad Actor Provisions:

1. AI shall not be utilized to create "deepfake" or *deceptive* "synthetic media" content.
   a) For "deepfakes" and "synthetic" media to be considered appropriate, the following will be adhered to:
      - Informed consent for the likeness and voice of individual depicted.
      - Audiences must be clearly informed that content they are viewing or hearing has been generated or altered by AI through labels, watermarks, or clear disclaimers.
      - The purpose of the content must be constructive and ethical and not deceptive, harmful, or contain misinformation.
2. Reporting and Response: Establish a mandatory reporting system for suspected AI misuse, with Departments defining their own reporting processes and response teams.
3. Unauthorized or inappropriate use of AI may result in disciplinary action up to and including termination

X. Security and Compliance:

1. Security Rules for Public and Proprietary GenAI: Compliance with established security administrative policies and procedures for data management and application development is required, with Departments able to impose stricter controls as needed when approved by the IT Department.
2. Monitoring and Reporting: Potential security concerns should be reported to IT and policy violations in AI use should be reported to HR as soon as possible.
3. Employees using AI remain responsible for ensuring compliance with county administrative policies.
4. AI tools must comply with Storey County's cybersecurity policies.
5. No sensitive government or citizen data shall be shared with AI platforms that do not meet county security standards.
6. Any AI-related processes affecting the public must be disclosed, ensuring transparency.
7. The county will implement regular reviews of AI systems to ensure their fairness, accuracy, and compliance with legal and ethical standards.
8. Any task or process automated using AI must be documented, including the role of the AI tool and its expected outcomes.
9. AI tools shall only use high quality, accurate, and relevant data to ensure reliable outcomes. Employees are responsible for validating the data input into AI systems.
10. Employees must have the data used in AI processes according to the county's data security policies. Any AI system used will only have access to data that is necessary for the function to minimize the exposure to sensitive information.
11. Secondary factory user authentication may be implemented.
12. When using third party and solutions, employees must ensure that vendors adhere to the county's security, privacy, and ethical standards. Vendors should provide transparency on how their AI tools function. Employees must monitor the performance and compliance of third-party AI tools regularly and report any potential issues to management.

XI. Implementation Plan:

1. AI Action Plan: Develop and implement a comprehensive plan that aligns with NIST's AI Risk Management Framework, including:
   a) Establishing policies, processes, standards, and contracts for AI tools.
   b) Embedding risk-based assessments into county processes.
   c) Ensuring monitoring and legal analyses of AI tools as needed.
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.
    a) Safety training for all personnel involved in AI operations will be provided as it becomes available.
4. County employees will be provided with updates on policies and practices as needed/changes are made.
5. Ongoing education on AI advancements and responsible implementation will be provided as needed.

XII. Data Handling Protocols:

1. Data Classification: Make groups for different types of data, like aggregate, de-identified, and anonymous. Have rules on how to handle each type to keep information safe and private.
    a) Aggregate data is data that has been collected and combined from multiple sources or individuals to create a summary or overview of a larger population or group.
    b) De-identified data refers to information where all personally identifiable information (PII) and protected health information (PHI) has been removed, making it impossible to link the data back to an individual.
    c) Anonymous data is information that cannot be linked to a specific individual or entity.
2. Data Protection Standards: Require all AI systems to adhere to stringent data protection standards, including encryption and access controls.

XIII. Threat Identification and Mitigation:

1. Regular Assessments: IT to conduct regular security-risk assessments, with Departments conducting additional assessments as needed.
    a) A security risk assessment (SRA) is a process that identifies, evaluates, and prioritizes potential vulnerabilities and threats to an organization's information systems, data, and operations.
2. Mitigation Strategies: IT to develop strategies to address identified risks, allowing Departments to implement additional strategies based on their specific risk profiles.
    a) A mitigation strategy is a plan of action designed to reduce or eliminate the impact of potential risks or threats.

XIV. Auditing:

1. Compliance: Departments must report AI-related incidents and participate in audits with flexibility as needed.
2. Audit Reporting: Document findings and develop action plans based on audit results.

XV. Continuous Reporting:

1. Feedback Mechanisms: Regularly review feedback from employees, stakeholders, and residents to inform them of policy updates, allowing IT in conjunction with Departments and HR to establish their own feedback mechanisms.
2. Policy Updates: This policy will be reviewed and updated annually, with Departments encouraged to update their own policies based on evolving needs.

XVI. Compliance:

All county departments 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.

XVII. Responsibility for review:

The County Manager, or their designee, will review this policy every 5 years or more frequently if necessary.