POLICY NO.:	**903**	TITLE:	**Artificial Intelligence (AI) Acceptable Use**
EFFECTIVE:	March 6, 2026	REPLACES:	
APPROVED:			

A. Purpose

1. Artificial intelligence (AI) has rapidly transformed the delivery of public services and the internal operations of city government. This policy guides the responsible, ethical, and secure integration of AI systems—both generative and non-generative—across all departments and functions of the City of Springdale.

2. Grounded in principles of transparency, accountability, equity, privacy, and resilience, this policy ensures that AI technologies benefit residents, maximize operational efficiency, and uphold public trust, while protecting against operational, ethical, security, and legal risks.

B. Scope

1. This policy applies to all employees, interns, consultants, contractors, vendors, and volunteers working for, or on behalf of, the City of Springdale. It also applies to anyone procuring, deploying, developing, configuring, managing, or operating AI solutions as part of official city duties.

2. AI systems covered by this policy include but are not limited to:

    a. Generative AI platforms (e.g., chatbots, automated content creation)

    b. Automated decision-making systems

    c. Machine learning analytics

    d. Predictive algorithms

    e. Robotic process automation (RPA)

    f. Smart city infrastructure (IoT, camera analytics, allocation modeling)

C. Definitions

- **Artificial Intelligence (AI):** Machine-based systems that analyze data, make decisions, give recommendations or predictions, and influence real or digital environments through automated processes. This includes generative models, neural networks, supervised/unsupervised ML models, and expert systems.

- **Generative AI:** Automated systems that produce new content, text, audio, images, or code, based on learned patterns and user input.

- **Automated Decision-Making:** Algorithms that reach conclusions or make choices based on predefined logic, potentially affecting eligibility, service delivery, or public impact.

- **AI System Owner:** The department or designated individual accountable for any AI deployment, its ethical use, maintenance, performance, and compliance with this policy.

D. Guiding Principles

1. Transparency

   a. All use of AI—especially those impacting residents, public information, or City service delivery—must be openly communicated. Applications with public interfaces must indicate "AI-generated" or "Automated Decision-Making" wherever relevant.

   b. Departments shall document AI system purposes, decision logic, and data usage, and make appropriate disclosures to stakeholders and affected persons, if applicable.

   c. Documentation shall include model type, training data (where feasible), provenance, and explainability notes. These records enable future audit, governance, and public inquiry.

2. Accountability

   a. Where AI informs, augments, or automates decision-making impacting City operations or residents, a designated human reviewer must validate outcomes before actions are finalized.

   b. Departments must maintain clear accountability for system management, data inputs, and outputs. Mistakes, biases, or errors must be reported immediately to the IT and risk teams.

   c. When AI outputs are wrong or undesirable, City staff must override and correct them, documenting the reasoning.

3. Fairness, Bias Mitigation, and Equity

    a. AI systems must be routinely evaluated for bias, discrimination, or disparate impact, especially in functions relating to citizen eligibility, resource distribution, hiring, law enforcement, or public safety.

    b. City staff must ensure that model training data, algorithm selection, and system outcomes are reviewed through an equity lens.

    c. No AI system may perpetuate discrimination or systematic exclusion based on race, ethnicity, gender, disability, age, socioeconomic status, or other protected characteristics.

4. Privacy and Data Protection

    a. All AI systems must comply fully with federal, state, and city privacy mandates (e.g., HIPAA, FERPA, GDPR where applicable). No personally identifiable, sensitive, or confidential data may be entered into any commercial, cloud-based, or third-party AI tool unless approved for such use.

    b. AI models should utilize data minimization, de-identification, or anonymization. Raw sensitive data must never be used for training, inference, or sharing unless specifically authorized by city legal or privacy officers.

    c. Third-party AI vendors and platforms must comply with the City's data governance, retention, and privacy policies, including contractual agreements specifying data rights, protections, and breach notifications. No data may be sold or transferred without expressed consent of the City of Springdale.

5. Cybersecurity and System Resilience

    a. All AI platforms, systems, and apps must be reviewed and approved by the City IT Department and comply with City cybersecurity protocols, including risk assessments, penetration testing, and compliance checks.

    b. System architectures must minimize attack surfaces and ensure robust authentication, logging, and incident response capabilities.

    c. Timely updates, patch management, and model retraining are required to ensure ongoing system performance and security.

6. Reliability, Explainability, and Validation

a. Departments must validate the performance, reliability, and accuracy of their AI systems for their intended uses. AI models must be regularly tested against known data and use cases.

b. Outputs must be explainable: staff and affected persons should be able to understand in clear, non-technical language why an AI system made a recommendation or decision.

c. Unexplained or "black box" model outputs are unacceptable in critical or high-impact workflows.

7. Human Alternatives, Review, and Intervention

    a. In all cases, human employees retain final authority to override, modify, or halt AI-driven recommendations and decisions.

    b. AI systems must include avenues for feedback, appeal, and correction from both staff and the public.

    c. City staff must be trained to challenge AI system results, escalate concerns, and facilitate human-in-the-loop (HITL) oversight.

8. Collaboration, Training, and Innovation

    a. The City encourages responsible AI innovation to meet community needs. Department heads and IT will provide ongoing and role-based training in responsible AI use, risk management, and escalation procedures.

    b. City partnerships with private, public, and academic organizations to advance understanding, testing, and improving AI systems are encouraged.

    c. Employees must keep abreast of evolving best practices and emerging risks and integrate learning into daily operations.

E. <u>Acceptable Uses</u>:

1. Automating repetitive and low-risk internal tasks (e.g., scheduling, information sorting, data processing).

2. Improving service delivery (e.g., traffic modeling, resource allocation).

3. Enhancing public communication (chatbots, information portals), provided AI-generated content is validated by City staff.

4. Augmenting data analytics and forecasting, subject to regular audit.

5. Personalized resident services and accessibility features (where oversight is maintained).

F. Prohibited Uses

1. Automated, non-reviewed determinations in areas affecting legal rights, eligibility, benefits, or disciplinary measures.

2. Surveillance, facial recognition, or emotion/sentiment analysis except as explicitly authorized by law and City approval.

3. Creating, spreading, or amplifying misinformation, disinformation, or deepfakes.

4. Manipulating official records, data, or public messaging without disclosure and validation.

5. Processing or disseminating personally identifiable information without explicit authorization by the privacy officer and legal counsel.

G. Procurement and Approval

1. All Departments must obtain IT and Administrator approval before acquiring or deploying any new AI tool.

2. Procurement must include due diligence for vendor reliability, model transparency, data security, and contractual compliance.

H. Incident Management

1. Suspected misuse, bias, error, or system failure must be reported immediately.

2. Incidents will be investigated by the Department Director with corrective actions documented.

3. Breach or compromise of data by an AI system follows the city's standard cybersecurity incident reporting protocol.

I. Governance and Enforcement

1. Enforcement is the responsibility of department heads, city IT, and HR.

2. Violations of policy—intentional or negligent—result in sanctions, including removal of AI access, disciplinary action, or notification to legal/regulatory agencies as required by law.

3. Routine and random audits will be undertaken. Appeals and correction processes are documented and available for staff and public concerns.