city of albuquerque

ONE ALBUQUERQUE technology & innovation

ARTIFICIAL INTELLIGENCE POLICY 2025

TABLE OF CONTENTS

INVITED WORKING GROUP MEMBERS

Director Mark Leech	Department of Technology and Innovation
Jeff Hertz	City Council Services Department
Shanna Schultz	Mayor's Office
Ethan Watson	City Clerk's Office
Cristobal Rocha	City Clerk's Office
Deputy Chief J.J. Griego	Albuquerque Police Department's Real Time Crime Center
Saif Ismail	General Services Department, Energy & Sustainability Management Division
Ian Stoker	Human Resources Department
Sonya Lara, Jacky So	Office of Equity and Inclusion
Alan Heinz, Ian Alden	Legal Department
Michelle Gricius, Jon ZuVerink	Planning Department, Albuquerque Geographical Information Systems Division
Kathleen Oney, Eddie DeHerrera	Department of Finance and Administration, Purchasing Division
Chris Sylvan	City of Albuquerque's Information Services Commission
Shaun Willoughby	Albuquerque Police Officers' Association (APOA)
Sonya Lara, Jacky So	Office of Equity and Inclusion
Joel Villareal	American Federation of State, County and Municipal Employees (AFSCME)
Cpt. Noah MacGillivray	International Association of Fire Fighters (IAFF) Local 244
Sonia Gipson Rankin	Civil Rights Advocate
Jeron Campbell	Civil Rights Advocate
Kenneth Ingham	Community Member
Aaron Roth	Community Member
Brian Osterloh	Software Vendor
Annemarie Henton / Brady Key	Software Vendor
Alex Webb	University of New Mexico Department of Computer Science
Brian Rashap	Central New Mexico Community College (CNM)
Mueen Abdullah	University of New Mexico Department of Computer Science
Melanie Moses	University of New Mexico Department of Computer Science

ARTIFICIAL INTELLIGENCE POLICY

PURPOSE

Artificial Intelligence (AI) is a powerful technology with the potential to transform the City of Albuquerque, positioning us at the forefront of innovation and thought leadership in artificial intelligence. The widespread adoption of AI must be done with thought and care.

Vision: The City of Albuquerque will be a national leader in the responsible and sustainable use of AI to advance community well-being in ways that are transparent, equitable, accountable, secure, and adaptable.

Mission: To create a community-centered ecosystem that values responsible innovation while leveraging cutting-edge technology to improve lives, enhance public services, preserve public trust, and is rooted in our shared values of access, advancement, and accountability.

SCOPE

All City departments, employees, vendors, contractors, and volunteers who operate on behalf of the City of Albuquerque are subject to this policy.

STANDARDS FOR ETHICAL USE OF ARTIFICIAL INTELLIGENCE: CODE OF ETHICS

The Code of Ethics establishes the core principles that guide this policy to ensure artificial intelligence (AI) is used in ways that balance innovation with public safeguards and trust.

- **Innovation:** The City values innovation and will responsibly explore AI technologies that enhance services, benefiting people, the community, and the environment.
- **Transparency, Explainability, and Interoperability:** AI use must be communicated. Systems should disclose model type, training source, and legal access to data. When complete transparency isn't feasible, limitations must be documented. AI systems should be able to justify their outputs and recommendations accurately. AI systems must integrate effectively with City information technology infrastructure, including seamless data input and output.
- **Safety, Security, and Validity:** AI must be used safely, minimizing potential to harm human life, property, or the environment. AI systems must not leak or export sensitive data outside City control. This includes taking all reasonable steps to prevent internal leaks of highly sensitive information (e.g., HR, health, or other PII). Systems must comply with City data protection standards. AI use must be monitored to ensure that it produces correct results (not hallucinations) and avoids unexpected failures, degrading gracefully, at worst. AI tools must undergo testing before acquisition and use to maximize safety, validity, and reliability.
- **Fairness, Bias, and Risk Awareness:** AI systems must be fair, with bias actively managed and mitigated. While complete elimination of bias may be unachievable, vendors must be questioned on their mitigation strategies. When evaluating new services, software, or platforms, the City must identify and assess potential risks and impacts related to AI use.
- **Ethical Use and Human-Centered:** Once other principles are met, AI should be used to enhance staff efficiency and improve citizen services. City staff and contractors must consider the impact of AI use on individuals. When uncertain, they should revise their approach or seek additional input.

POLICY

1. **Data Privacy**

   1.1 All AI tools shall follow the City's existing data governance policies.
   1.2 Departments shall disclose what data is collected, how it is used, and for what purpose. The use of new or sensitive data types may trigger additional reviews, such as privacy impact assessments or internal reviews.
   1.3 AI systems must comply with DTI cybersecurity standards, including authentication, encryption, and endpoint protection.
   1.4 AI use shall enhance, not bypass, City security protocols and privacy obligations.
   1.5 Employee and vendor accountability shall be embedded through standard compliance measures, including training, contracts, and audit mechanisms.

2. **Harm and Bias Mitigation**

   2.1 The City shall maintain an AI Code of Ethics that establishes fundamental principles for the use of AI, including human oversight and accountability for all work generated with or supported by AI. All depart-

ments shall acknowledge that AI tools may perpetuate bias based on training data and are required to actively mitigate the risk of reinforcing harmful stereotypes or discrimination.

2.2 The City adheres to a model of responsible innovation. All AI pilot programs shall follow ethical experimentation guidelines, include clearly defined intended use cases, assess impacts on departmental operations, staff, and community members, and incorporate a revision process informed by pilot findings.

2.3 AI use is intended to augment, not replace, human decision-making. Departments shall define acceptable levels of automation and establish procedures for required human review. City employees are responsible for the content, accuracy, appropriateness, and tone of all work products generated with the assistance of AI.

2.4 The City shall enforce structural safeguards to ensure the responsible use of AI, including the mandatory documentation of AI workflows and the disclosure of AI integration in any public-facing services provided by the City.

3. Public Records Management

3.1 All departments are required to document decision-making criteria and procedures for human oversight when using AI tools.

3.2 Departments must maintain records sufficient to comply with the retention schedule as adopted by the city.

4. Acquisition and Use of AI Technology

4.1 Only City-approved AI systems may be used, and a list of authorized tools will be maintained. Access is granted by DTI in coordination with department heads. AI use must include human-in-the-loop oversight to ensure accountability and transparency.

4.2 All new AI tools shall undergo a DTI-led risk assessment, which evaluates data privacy, cybersecurity, and bias risks. DTI, with input from departments and legal counsel, will define data quality and bias assessment standards for the approval of tools. Tools that fail the assessment may not be used unless remediated. An escalation pathway for unresolved risks will be routed through existing City governance structures.

4.3 All AI tools should undergo regular risk assessments coordinated by DTI, including evaluations of ethical impact, data protection, and potential unintended consequences. Systems with higher risk profiles shall be subject to more frequent review. Success criteria for bias and risk mitigation shall reference current industry standards and civil rights benchmarks. Lessons learned during implementation shall inform ongoing policy updates, and DTI will identify, evaluate, and share promising and ethical AI applications.

5. Education and Training

5.1 All City employees must be trained on the ethical and responsible use of AI. The Administration should develop a rule or instruction to ensure new and existing employees receive foundational training on AI fundamentals and ethics. Staff must complete training before gaining access to AI tools and sign an “Ethical Use of AI” agreement.

5.2 All training efforts will be consolidated under a unified Training & Literacy strategy overseen by an independent board to ensure consistency across departments. The City will identify and collaborate with external partners to develop online tools and resources that support ongoing staff learning.

5.3 As technology evolves, staff will be regularly informed about emerging risks, new tools, and the most up-to-date best practices.

5.4 The City will collaborate/engage with external partners to offer publicly available in-person or virtual sessions on AI literacy and responsible use of AI.

6. Governance

6.1 The City's use of AI shall be governed in accordance with all applicable federal, state, and local laws, regulations, rules, and ordinances, as well as City policies and departmental rules.
6.2 DTI shall coordinate an inventory for departments to report current and planned AI tools, including those in use, under development, or in pilot stages.
6.3 DTI shall lead a standardized assessment process in collaboration with departments to identify current and potential AI use cases, determine upskilling and reskilling needs, develop department-specific AI wish lists, and analyze implementation costs related to staffing, training, maintenance, and compliance.
6.4 DTI shall develop a citywide AI Integration Plan to establish procurement standards and ethical guidelines for evaluating third-party tools, prevent redundancy and fragmentation, and define AI categories (e.g., generative, predictive, decision-support) with proportionate governance.
6.5 The City shall maintain formal structures to facilitate interdepartmental collaboration on AI implementation, review, and the sharing of best practices within the City.
6.6 To ensure AI use improves public services, DTI and departments shall explore how AI can streamline workflows, enhance service delivery, while bearing in mind the importance of human input, judgment, and valuing the importance of human labor.
6.7 DTI shall publish information about AI use within the City on cabq.gov and maintain a public feedback form for questions and suggestions.
6.8 This policy will be subject to public comment before its initial adoption, but is not an act of rule-making. Post-enactment revisions may or may not be subject to public comment.

NON-COMPLIANCE

Violations of this policy may result in disciplinary action consistent with employment rules and expectations generally applicable to all City Employees.

RELATED POLICIES AND STANDARDS

Cybersecurity Policy
IT Policies, Standards, and Procedures

RESPONSIBILITIES

This AI Policy will be reviewed and updated periodically to reflect the evolving nature of AI tools, resources, and applications.

AI POLICY MISSION STATEMENT

VISION

The City of Albuquerque will be a national leader in the responsible use of AI to advance community well-being in ways that are transparent, equitable, accountable, secure, and adaptable.

MISSION

To create a community-centered ecosystem that values responsible innovation while leveraging cutting-edge technology to improve lives, enhance public services, preserve public trust, and is rooted in our shared values of access, advancement, and accountability.

PRIORITIZATION MATRIX

The working group recommends adopting a systematic evaluation framework to assess and prioritize AI implementations based on potential impact and risk. This matrix evaluates proposed AI use cases across three key dimensions: severity of potential harm, individuals' ability to opt out, and public impact. The matrix uses mandatory screening criteria to ensure all AI tools enhance public services, maintain human oversight, and comply with established policies. Each dimension is scored to determine a total priority level (low, medium, or high), enabling the City to direct appropriate resources and oversight to higher-risk or higher-impact projects while streamlining approval for lower-risk applications.

The City of Albuquerque is committed to the responsible and equitable adoption of AI technologies. This matrix helps identify which tools require additional review and monitoring, as well as whether specific AI use cases should be prioritized, based on three key dimensions.

- Severity of Potential Harm
- Ability for Individuals to Opt Out
- Public Impact

PRIORITIZATION MATRIX

Screening Criteria (Basic Eligibility)

Use these criteria to determine if an AI use case is appropriate.

- Purpose: Does the use support a public service or operational improvement?
- Data Availability: Is the required data accessible and representative?
- Compliance: Does the use comply with policy and standards?
- Human Oversight: Can a human remain in the loop?

If yes to all, proceed to the matrix.

HOW TO USE THE MATRIX

1. For each use case, assign scores across the dimensions of the criteria.
2. Add the total to determine the priority score. Score range: 3–9.

- High Priority: 7–9 points
- Medium Priority: 5–6 points
- Low Priority: 3–4 points

EXAMPLE USE CASE: MULTILINGUAL SERVICE BOT FOR 311

Severity of Potential Harm	Opt-Out Available?	Public Impact	Total Score
2	2	3	7

Priority Category	Severity of Potential Harm	Opt-Out Available?	Public Impact	Review Requirements
HIGH 3 POINTS	Low impact; outputs are advisory or easily reversible; minimal risk of harm	Yes, full opt-out	Broad public benefit	Full AI Review, AIA Form, AI FactSheet, Data Usage Protocol, Public Engagement, Annual Monitoring, Review as needed
MEDIUM 2 POINTS	Affects individual well-being or service access; moderate reversibility	Limited or unclear opt-out	Improves operations	AI Review, AIA Form, AI FactSheet, Targeted Engagement, Internal Approval, Annual Monitoring
LOW 1 POINTS	Impacts health, civil rights, legal status, economic access, or public safety; irreversible or long-lasting consequences	No opt-out	Minimal	Internal Documentation, Optional Monitoring

DEFINITIONS OF KEY AI TERMS

Accountability - a property that ensures that actions of an entity can be traced uniquely to the entity (systems context); the obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept the responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner

In tandem with AI accountability - the idea that artificial intelligence should be developed, deployed, and utilized such that responsibility for bad outcomes can be assigned to liable parties (AI Accountability, n.d.).

Algorithmic Discrimination - occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, skin color, national or ethnic origin, cultural group, language, gender identity or expression, sexual orientation, mental or physical ability, age, religious or political opinion or activity, economic status, immigration status, or housing status

Artificial Intelligence (AI) - type of computer science that deals with computer systems that perform tasks which usually require human intelligence, such as reasoning, problem solving, perception, and language. AI is classified into three types based on capability:

- **Artificial Narrow Intelligence (ANI):** Specialized in a single task (Examples: Siri, Alexa, and recommendation algorithms for streaming platforms)
- **Artificial General Intelligence (AGI):** A theoretical system with human-like intelligence that can learn and apply knowledge across domains
- **Artificial Superintelligence (ASI):** A hypothetical AI that surpasses human intelligence in all respects

AI can also be classified by its functionality, which includes how it processes information, learns from data, and responds to its environment.

- **Reactive Machines:** No memory or learning; respond only to current inputs.
  Example: Netflix recommendation engine
- **Limited Memory AI:** Learns from recent data to improve performance.
  Examples: Alexa, Siri, self-driving cars, ChatGPT, Dall-E, smart home devices
- **Theory of Mind AI:** A future stage of AI that can understand and respond to human thoughts and emotions.
  Example: Early-stage research only
- **Self-Aware AI:** Hypothetical AI with consciousness and self-awareness.

AI includes technologies that enable machines to learn, reason, and make decisions.

- **Machine Learning (ML):** Enables systems to learn from data, identify patterns, and improve without explicit programming.
  Example: Fraud detection, Google Maps, Zoom Automated Captions and Cloud Recordings with Transcripts, Microsoft Teams Live Captions and Transcripts, and Webex Real-Time Transcription

- **Deep Learning:** A subset of machine learning using neural networks to process complex data and make advanced decisions.
  Example: Facial recognition
- **Natural Language Processing (NLP):** Enables machines to understand and generate human language in text or speech.
  Example: ChatGPT, Google Assistant, Zoom Automated Captions and Cloud Recordings with Transcripts, Microsoft Teams Live Captions and Transcripts, and Webex Real-Time Transcription
- **Computer Vision:** Utilizing deep learning techniques enables machines to interpret and analyze visual information.
  Example: Facial recognition
- **Robotics:** Applies AI to physical machines, enabling perception, decision-making, and action.
  Example: Surgical robots, warehouse automation
- **Expert Systems:** Simulate human expert decision-making using rules and data analysis.
  Example: Medical diagnostics
- **AI in Gaming:** Drives adaptive, intelligent behavior in game characters and environments.
  Example: Realistic non-playable characters (NPCs) in video games

Auditing - referring to AI definition; the assessment of an AI system and its supporting algorithms following secure, legal, and ethical standards. Assessment centers on whether or not it engages in prohibited activities, leans toward illegal bias, and/or introduces unacceptable risks

Bias - In tandem with AI bias, machine learning bias and algorithm bias; the occurrence of biased results due to human biases that skew the original training data or AI algorithm leading to distorted outputs and potentially harmful outcomes

Bias Reduction - referring to AI definition; the process of identifying and mitigating biases within AI systems to ensure fair and accurate decision-making. This involves addressing biases that can be present in the training data, the algorithms themselves, or the way the AI is deployed (Holdsworth, 2023)

Data Privacy - also known as information privacy; the principle that a person should have control over their personal data. This includes the ability to decide how organizations collect, store and use their data (Gomstyn & Jonker, 2024). In tandem with AI Privacy - the practice of protecting personal or sensitive information collected, used, shared or stored by AI. It addresses the need to protect individual data rights and maintain confident

Data Security - referring to AI definition; the practice of protecting the data used by AI and machine learning systems from unauthorized access, manipulation, and breaches. It involves implementing various security measures to safeguard sensitive information and ensure the integrity and availability of AI models and workflows

Discrimination - the biased or unfair treatment of individuals or groups by AI systems. This bias can manifest in AI systems making decisions or providing outcomes that disadvantage, exclude, or misrepresent certain groups of people

Documentation - the creation and maintenance of detailed records and materials about AI systems, models, datasets, and related processes

Ethical Use - in tandem with AI Ethics; the principles that govern AI's behavior in terms of human values. AI ethics helps ensure that AI is developed and used in ways that are beneficial to society. It encompasses a broad range of considerations, including fairness, transparency, accountability, privacy, security, and the potential societal impacts

Governance - the processes, standards and guardrails that help ensure AI systems and tools are safe and ethical. AI governance frameworks direct AI research, development and application to help ensure safety, fairness and respect for human rights

Hallucination - a phenomenon wherein a large language model (LLM), often a generative AI chatbot or computer vision tool, perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate. It is a common cause of AI-generated misinformation and occurs when AI algorithms produce outputs that are not based on training data, are incorrectly decoded or do not follow any identifiable pattern.

Large Language Models (LLM) - a type of artificial intelligence program that can understand and create text. It learns from a vast amount of data, often gathered from the Internet, which helps it recognize human language and other complex information

Misinformation - false information that is not purposely created to deceive others, but rather is caused by errors

Oversight - referring to AI definition; the mechanisms and processes in place to ensure that AI systems are developed, deployed, and used responsibly and ethically. This includes having human intervention and monitoring at various stages of the AI lifecycle, from design to deployment, to ensure that AI systems operate within defined ethical boundaries and societal values

Procurement - the leveraging of advanced technologies and algorithms to automate and enhance various procurement tasks, ultimately improving efficiency, accuracy, and decision-making. By analyzing large datasets, AI can identify patterns, predict future trends, and optimize processes, leading to cost savings, improved supplier relationships, and better resource allocation

Public Trust - referring to AI definition; the extent to which the public believes and relies on AI systems to act in their best interests and with integrity. It's a crucial factor for the successful adoption and integration of AI into various aspects of society (Afroogh et al., 2024)

Transparency - referring to AI definition; the understanding of how artificial intelligence systems make decisions, why they produce specific results, and what data they are using. This is done in order to help people understand and trust how these systems work

INVENTORY OF CURRENT AI PRACTICES OF CITY DEPARTMENTS

Purpose	Product	Department(s)	Benefits	Costs
Improve/Correct writing, generate first drafts	Various generative AI tools such as ChatGPT, Gramerly, MS Copilot, and Hootsuite AI tool	Various	Faster customer response	None
Translation of text	Various traslation AI tools such as Google Translate, Wordly, and MS Translate	Various	Faster customer response	None
Creation and editing of photo and video content	Various image generator tools such as Adobe AI, canva, designrr, and photoart	Various	Quicker image generation, better quality production	Depends on service
Transcription of text	Various transcription AI tools such as Zoom transcription, Otter.AI	Various	Faster customer response	Depends on service
Automated assistance with CAD designs	AutoCAD	GSD	Reduces design errors and costly rework	$2184.56/yr
Automation for design drawings	Bluebeam	GSD	Accelerates project timelines	$439.14/yr
Summarizing input from user-added stickies	Miro	Planning	Enhances project management	$2,000/yr
Summarize input from user-added comments (public facing)	Konveio	Planning	Increases community engagement and transparency	$14,000/yr
Patient survey, capturing vital signs via cell phone camera	Good Sam	AFR Alarm Room	Coordinates emergency response resources	$120,000
Simulate a variety of patient conditions to train in EMS	iSimulate	AFR EMS Training	Provides cost-effective training simulations	$7,740
One source information and planning for passengers	Dash2Virtual Assistant	Aviation	Ease of travel	$95,525
Investigative data analysis platform	Peregrine	APD	Faster intelligence gathering and case connections	None for AI components
OBRD Transcription	AXON	APD	Improves transparency	None for AI components
Facial recognition tool using large image databases	Clearview AI	APD Investigation	Faster intelligence gathering	None for AI components
Officer performance and conduct tracking system	Benchmark Analytics	APD Compliance	Improves accountability	None for AI components
Digital forensics for extracting data from phones and devices	Cellebrite	APD Investigation	Faster intelligence gathering	None for AI components

COMMUNITY ENGAGEMENT PLAN

The working group recommends adopting community engagement protocols to ensure residents have meaningful input into how artificial intelligence is implemented in city operations. Grounded in principles of transparency, equity, participation, reciprocity, and accessibility, the framework calls for proactive information sharing about AI use, early consultation with the public before decisions are made, and ongoing dialogue that amplifies voices from underrepresented communities. Public participation would be facilitated through monthly Emerging Technology Board meetings, a dedicated webpage with policy documents and training materials, and accessible communication in multiple languages and formats. The City would also commit to reporting back on how community feedback shapes AI projects and addresses resident concerns.

Grounded in principles of transparency, equity, participation, reciprocity, and accessibility, the framework calls for proactive information sharing about AI use, early consultation with the public before decisions are made, and ongoing dialogue that amplifies voices from underrepresented communities.

Community Engagement Principles

TRANSPARENCY

The City commits to proactively sharing information about how AI tools are used, the data involved, and the rationale behind the decisions. This includes publishing policy documents and training materials.

EQUITY

AI tools, policy, and engagement must prioritize inclusive processes that reflect the perspectives of underrepresented communities.

PARTICIPATION

Community input must be sought early, not after decisions are made. Input from residents is crucial, especially for those most directly impacted by AI tools.

RECIPROCITY

Engagement must be mutual. The City will close the loop by reporting back how community input shaped projects and how concerns were addressed.

ACCESSIBILITY

AI engagement must meet standards for linguistic, cultural, physical, and digital accessibility. Information must be presented in plain language, available in multiple languages, and various formats.

Community Engagement Mechanisms

- Emerging Technology Board (ETB) Meetings: The ETB will hold monthly public meetings, with time allocated for public comment. Meeting agendas and minutes will be published online.
- Webpage on cabq.gov: A webpage will host ETB materials, meeting notices, policy documents, updates, community training materials, and engagement opportunities.
- AI Use: The City will maintain a public-facing overview that offers information about AI tools being used across departments.

INTEGRATION OF AI INTO THE OPERATIONS OF CITY GOVERNMENT

The working group recommends adopting a framework to responsibly integrate artificial intelligence into municipal operations, prioritizing transparency, equity, and public benefit. The framework establishes clear procedures for evaluating, procuring, and deploying AI across departments, with mandatory oversight by an Emerging Technologies Board and safeguards, including human review, bias mitigation, and public disclosure. Through workforce training, ethical standards, and active community engagement, it ensures AI strengthens city services while protecting residents' rights and upholding democratic accountability.

INTEGRATION PROCEDURES

Workforce Readiness

- Identify roles and functions that AI systems may impact.
- Conduct readiness assessments and identify skills gaps across departments.
- Develop and implement upskilling and reskilling plans for staff affected by changes.
- Provide training tools and support mechanisms to address challenges introduced by AI integration.

Ethical Use and Bias Mitigation

- Apply AI Code of Ethics to all related activities.
- Require human-in-the-loop oversight for AI systems.
- Conduct both pre- and post-deployment risk assessments, including bias mitigation protocols.
- Ensure systems undergo legal and regulatory review prior to deployment.

Procurement

- Integrate AI considerations into procurement processes, including system architecture and design.
- Conduct a readiness assessment and develop necessary data systems before acquisition.
- Require safety, fairness, and alignment evaluations for all AI tools.
- Mandate pilot programs and community impact assessments prior to implementation.
- Use a standardized review and approval process for AI procurements

Product Review and Pilot Programs

- Evaluate AI products for performance, bias, and public impact before adoption.
- Pilot all new systems in controlled environments with defined success metrics.
- Conduct technical and security testing prior to full deployment.
- Require oversight from the Emerging Technologies Board for major purchases involving AI capabilities.

Transparency

- Maintain clear records in compliance with the New Mexico Inspection of Public Records Act (IPRA).
- Provide accessible public information and a feedback mechanism on cabq.gov.

Training and Education

- Require all employees using or procuring AI to complete onboarding and role-specific training.
- Partner with organizations such as InnovateUS and the New Mexico Technology Council to provide in-person and online learning opportunities.
- Require signed “Ethical Use of AI” agreements before granting staff access to AI systems.
- Regularly update training materials to reflect new tools, risks, and use cases.

Inclusive and Equitable Design

- Design all AI-supported services to ensure accessibility and benefit for all.
- Incorporate considerations for language access, cultural relevance, and digital inclusion.
- Uphold fairness and anti-bias standards throughout the AI lifecycle.

Emerging Technologies Board

To ensure ongoing oversight and responsible implementation, the City will establish an Emerging Technologies Board as a governance body to assess risks and impacts and uphold community transparency and accountability.

Responsibilities

- Guide and review all significant emerging technology decisions
- Foster collaboration across departments to address technological impacts
- Ensure that public and privacy rights, as well as equitable outcomes, are protected
- Regularly engage community stakeholders to gather input and address concerns
- Review, update, and enforce policies related to AI and emerging technologies
- Hear complaints regarding violations of AI or emerging technology policies
- Ensure procurements and uses of AI or emerging technologies are presented to the Board

TRAINING PLAN

In support of City of Albuquerque AI policy directed at regulating and implementing the integration of AI, a comprehensive foundational level setting must be achieved for existing and future employees so that everyone is approaching the conversation from an informed and equitable position. To that end, the working group Education and Training Committee articulated a tiered training approach which includes strategies for onboarding new employees as well as opportunities for continuing education for existing employees and leadership. Through the use of both online and in-person experiences, the working group envisioned collaborative engagements with entities such as Innovate(US), Central New Mexico Community College, and the New Mexico Technology Council.

In addition to internal protocols to instill AI literacy, the working group highlighted the importance of providing opportunities for the public to engage with AI and other emerging technologies. This regular civic interaction could incorporate speaker series and community workshops to provide both insight into new and emerging technology, and a forum for public discourse to ensure the continued productive exchange to ensure sustainable policy alignment around emerging technologies. The need to be heard by and seen as humans is fundamental to maintaining healthy and functioning communities as we carefully navigate the process of AI becoming more inextricably entwined with our daily activities and engagements.

PHASE ONE: CAPACITY BUILDING

Partnership Development

- Formalize partnerships through MOUs or collaboration agreements
- Create or identify AI educational content that aligns with the City's AI policy

Survey

- Assess AI skills, needs, and opportunities to inform curriculum development for training tiers and identify AI use cases

PHASE TWO: DEVELOP TRAINING PROGRAMS

AI 101: Literacy

- Build a common baseline understanding
- What AI is (and is not)
- Potential opportunities and challenges
- Key provisions of the City's AI policy
- Examples of AI use in government and community contexts

AI 202: Practical Applications

- Prompt engineering and effective AI queries
- Citation and source evaluation
- Risk assessment and bias mitigation
- Hands-on demos

Department-Specific Training

- Department meetings to review survey results and identify needs
- Tailored training based on workflows, responsibilities, and AI application "wishlists"
- Includes compliance, transparency, and risk management guidance

This regular civic interaction could incorporate speaker series and community workshops to provide both insight into new and emerging technology, and a forum for public discourse to ensure the continued productive exchange to ensure sustainable policy alignment around emerging technologies.

PHASE 3: ONGOING TRAINING AND EDUCATION

Continuous Learning

- Regular workshops on emerging AI tools, trends, and ethical considerations.
- Rotating "AI in Practice" showcase where departments share successes and lessons learned
- Annual public speaker series with local researchers, technologists, and ethicists

Transparency

- Regular review sessions with staff and community to evaluate policy relevance and application
- Opportunity for public feedback on AI applications in use and the use of emerging technologies by the City

Goals and Outcomes

- Leverage partnerships with local technology industry and educational institutions to create training content
- Build a shared AI foundation so staff start with the same baseline knowledge and can apply AI in compliance with policy
- Deliver tiered training that includes onboarding, continuing education, and leadership sessions in multiple formats
- Engage the public through forums on AI and emerging technologies to support transparent and trusted AI governance

CODE OF ETHICS

The Code of Ethics establishes the core principles that guide this policy to ensure AI is used in ways that balance innovation with public safeguards and trust.

- **Innovation:** The City values innovation and will responsibly explore AI technologies that enhance services, benefiting people, the community, and the environment.
- **Transparency, Explainability, and Interoperability:** AI use must be communicated. Systems should disclose model type, training source, and legal access to data. When complete transparency isn't feasible, limitations must be documented. AI systems should be able to justify their outputs and recommendations accurately. AI systems must integrate effectively with City information technology infrastructure, including seamless data input and output.
- **Safety, Security, and Validity:** AI must be used safely, minimizing potential to harm human life, property, or the environment. AI systems must not leak or export sensitive data outside City control. This includes taking all reasonable steps to prevent internal leaks of highly sensitive information (e.g., HR, health, or other PII). Systems must comply with City data protection standards. AI must be monitored to ensure that it produces correct results (not hallucinations) and avoids unexpected failures, degrading gracefully, at worst. AI tools must undergo testing before acquisition and use to maximize safety, validity, and reliability.
- **Fairness, Bias, and Risk Awareness:** AI systems must be fair, with bias actively managed and mitigated. While complete elimination of bias may be unachievable, vendors must be questioned on their mitigation strategies. When evaluating new services, software, or platforms, the City must identify and assess potential risks and impacts related to AI use.
- **Ethical Use and Human-Centered:** Once other principles are met, AI should be used to enhance staff efficiency and improve citizen services. City staff and contractors must consider the impact of AI on individuals. When uncertain, they should revise their approach or seek additional input.

PRIVACY & SECURITY PROTOCOLS

While artificial intelligence introduces new applications, it does not alter the fundamental principles of information security, privacy, and technology governance already established by the City. The City's existing cybersecurity and IT standards are intentionally comprehensive, designed to adapt to emerging technologies without requiring frequent revisions for each new tool or system. Rather than duplicating or fragmenting our governance structure, we have chosen to reference these current policies to ensure continuity, consistency, and alignment with the City's overarching security and operational standards and IT best practices.

Please note these links direct to eweb, which is only accessible while on City internet.

Cybersecurity Policy
IT Policies, Standards, and Procedures

CYBERSECURITY POLICY

EFFECTIVE DATE: March 9, 2022 | REVISED DATE: March 9, 2022

1. PURPOSE:

For the promotion of a secure computing environment for City of Albuquerque services and resources.

2. SCOPE:

Applies to all computing resources connected to the City's internal network.

3. POLICY:

The City of Albuquerque (City) shall promote a secure computing environment. This secure computing environment shall be deployed and maintained to meet applicable federal, state, local, and industry cyber security guidelines. As such, the City shall develop standards for: cybersecurity technology; electronic authentication; technology asset (hardware, application, and data) security; and employee cybersecurity education and testing. This policy and related standards shall be published online using terminology understandable to the broad user base.

4. ENFORCEMENT:

Violation of this policy shall be reported to the appropriate supervisor and may be subject to potential disciplinary action, up to and including termination.

5. EXCEPTIONS:

Limited exceptions to the policy may be granted by the Director of the Department of Technology and Innovation on a case-by-case basis.

6. DEFINITIONS:

a. Internal city network - A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. An internal network is typically organization-owned and may be organization-controlled while not being organization-owned.

7. RESOURCES:

Resources may be modified by the Technical Review Committee. Standards will be developed in accordance with the resources below. The city shall endeavor to maintain compliance with the following resources:

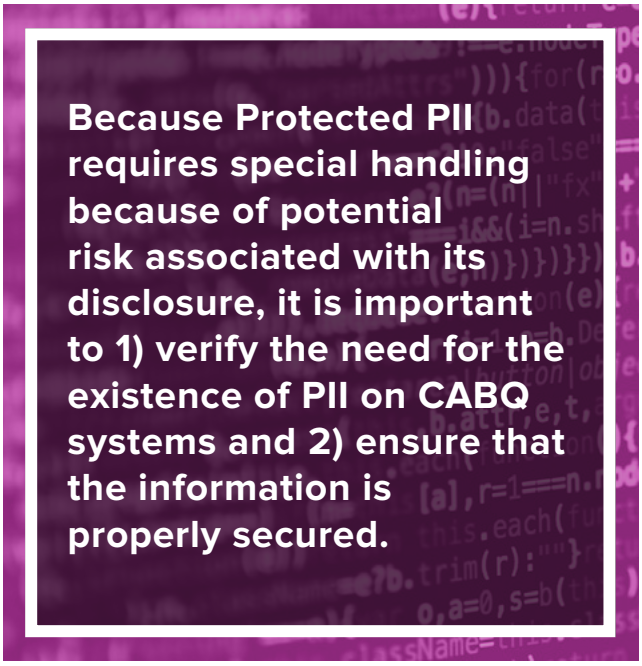
a. Payment Card Industry Data Security Standard - PCI DSS:
b. Health Insurance Portability and Accountability Act - HIPAA:
c. FBI Criminal Justice Information Services for Law Enforcement/Courts - CJIS:
d. National Institute of Standards and Technology: Information Technology - NIST:
e. International Organization for Standardization: Information Technology -
f. Information Systems Audit and Control Association (ISACA) - Good-Practice Framework:
g. Governance and Management of Enterprise IT, COBIT:

IT POLICY – PERSONALLY IDENTIFIABLE INFORMATION (PII) & SENSITIVE DATA

City of Albuquerque employees, in the course of their normal job responsibilities, will come into contact with Personally Identifiable Information (PII). It is important for employees to understand their roles in the collection and storage of PII.

1. PURPOSE:

The purpose of this policy is to protect City of Albuquerque's personally identifiable information and sensitive data from unauthorized disclosure and inappropriate use. This policy provides details on how to identify and handle Personally Identifiable Information (PII), the process of securely storing any PII that the organization is required to maintain, and what to do in the event of a disclosure of PII.



2. SCOPE:

All staff, employees, and entities working on behalf of the City of Albuquerque who are using City owned or personally owned devices that connect to the City's network are subject to this policy.

3. POLICY:

Identifying PII

There are two (2) types of Personally Identifiable Information (PII) and identification of each type will dictate the actions needed to ensure its safety and integrity. This includes citizens and employees

- **Public PII**
  This is information that is available in public sources such as telephone books, employee directories, public websites, etc. the following information can be considered Public PII:
    - First and Last Name
    - Address
    - Work Telephone Number
    - Work Email Address
    - Home Telephone Number
    - General Educational Credentials
    - Personal Email Address(es)
    - Photos and Videos
- **Protected PII**
  This is any information which, if lost, compromised, or disclosed without authorization, could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual. It includes one or more of the information outlined below:
    - Social Security Number
    - Username and Password
    - Passport Number
    - Alien Registration Number
    - Credit Card Number
    - Clearances
    - Banking Information
    - Biometrics
    - Date and Place of Birth
    - Mother's Maiden Name
    - Criminal, Medical, and Financial Records
    - Educational Transcripts*
    - Photos and Videos including any of the above

    **Note: Educational transcripts fall under FERPA guidelines, please see the FERPA Compliance Guidelines for details.*

Maintaining PII

During normal job responsibilities, employees may come in contact with either Public of Protected PII, either existing in the City of Albuquerque's network, or as part of a business process. Because Protected PII requires special handling because of potential risk associated with its disclosure, it is important to 1) verify the need for the existence of PII on CABQ systems and 2) ensure that the information is properly secured.

- **Verifying the need to collect PII**
  Best practice dictates that an organization only collects the least amount of information in order to follow standard business policies. Caution should be taken when collecting Protected PII. The need to collect the information should be periodically reviewed, and if deemed unnecessary, the policy should be altered to reflect the change.

- **Collection Policies**
  If PII needs to be collected, employees have certain responsibilities in making sure the data is secured. Any written information as a result of a phone conversation must be destroyed via shredding. Physical files that contain PII should be locked in a secure cabinet or room when not being actively viewed or changed. Any PII data collected should not be stored on the local workstation; it needs to live in a secure location where it can be encrypted and backed up.

- **Verifying the need to store PII**
  Whenever PII is found living in the City of Albuquerque's network, a determination needs to be made regarding whether the information is needed for an existing business practice, or if it can be securely disposed of. If the information needs to be retained, please contact the Department of Technology and Innovation Security Group for guidance on the best means to secure or dispose of the information properly.

- **Authorized Dissemination of PII**
  In the event an outside entity would need to have any data that includes Protected PII, said entity would need to confirm that they understand the sensitivity of the information, and the need to properly safeguard it. Once it leaves the City of Albuquerque, the DTI Security Group cannot guarantee its security. Transport of data should be done through secure means (ideally shared through encryption or other secured transport methods.)

- **Unauthorized Dissemination of PII**
  In the event of an unauthorized disclosure or access of PII:

    - Report the incident to your direct supervisor and to the DTI Security Group
    - Send an email to: ISDHelpdesk@cabq.gov
        - Do NOT forward any compromised information in the email
        - Include the location of the information (email or network location)
        - If email, include the sender and subject (unless the subject contains the PII)
        - Include any other relevant details, such as location and contact phone number
    - Comply with the instructions from the DTI Security Group

DTI PII Oversight

- DTI Security Group will meet monthly to review PII inventory with the Infrastructure Manager
- Infrastructure Manager shall notify DTI Security Group of any changes in PII systems.
- DTI Security Group shall insure the inventory is updated accordingly
- For non-DTI servers DTI Security Group shall review monthly with ISGG and Department Liaisons to ensure PII inventory.

4. SENSITIVE DATA:

The following items are examples of sensitive data, but are not limit to;

- Personal identification information such as:
    - Social Security Numbers,
    - Personal identification numbers which may be used other than Social Security
    - Number,
    - Employee home address,
    - Employee home telephone number,
    - Information protected by the Health Insurance Portability and Accountability Act of 1996
    - (HIPAA),
    - Information protected by the Family Educational Rights and Privacy Act (FERPA),
    - Information protected by the Payment Card Industry Data Security Standard (PCI DSS),
    - Information protected by the Federal Information Security Management Act (FISMA),
    - Credit card account numbers, expiration dates, and card verification values (CVV)
    - Bank account numbers (City, employee, vendor, etc.),
    - Computer system IDs and/or passwords.

5. STRATEGIC AND TACTICAL INFORMATION:

- This includes any data that is considered strategic to the City of Albuquerque and if compromised would provide an exploit to compromise security.

  Examples of strategic data include, but are not limited to;
  1. Telecom and Network diagrams,
  2. Infrastructure layouts,
  3. Server names and IP addresses.

- Neither this policy nor any part of this policy shall be construed to override federal, state, or City statutes and regulations on public information.

6. ENFORCEMENT:

This policy is for your protection. Violation of this policy could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

7. EXCEPTIONS:

Limited exceptions to the policy must be approved by the Director of the Department of Technology and Innovation

8. DEFINITIONS:

- Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, biometric records, etc... alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- FERPA: The Family Educational Rights and Privacy Act of 1974 sets forth requirements regarding the rights of students and the obligations of institutions to ensure the privacy and accuracy of education records.

IT POLICY - EMPLOYEE INTERNET USE

1. SCOPE:

City of Albuquerque employees access the Internet from City-owned computers and mobile devices. This access is intended for business-related purposes (such as communicating with customers, suppliers, and colleagues, to research relevant topics and to obtain useful business information).

2. POLICY:

Policy Definitions:

City of Albuquerque employees access the Internet from City-owned computers and mobile devices. This access is intended for business- related purposes (such as communicating with customers, suppliers, and colleagues, to research relevant topics and to obtain useful business information).

The public may access the Internet from City-owned computers at a number of public locations. The City provides Internet access as a service to our citizens. Access by library patrons is covered under the Library Computer Use Policy.

All existing laws and City policies apply to employee conduct when accessing the Internet on City-owned computers and mobile devices, especially those that deal with intellectual property protection, privacy, misuse of City resources, sexual harassment, data security, and confidentiality.

Policy Provisions:

- City Internet access is provided to employees for the purposes of study, research, service and other activ-

ities, which, with the exception of occasional de minimis personal use, must be for purpose of conducting official business or in support of the City's mission.

- Each City employee using the City's Internet access shall identify themselves honestly, accurately, and completely when corresponding or participating in online activities.
- City Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or local jurisdiction in any material way.
- Employees have no right of ownership or expectation of personal privacy as to their City Internet usage. It is possible to monitor Internet usage, and the City reserves the right to inspect any and all network traffic and files stored on City resources. The City reserves the right, without notice, to limit or restrict any employee's Internet usage.
- Offensive content may not be accessed, displayed, archived, stored, distributed, edited, or recorded using City network, printing, or computing resources. Offensive content includes, but is not limited to, pornography, sexual comments or images, profanity, racial slurs, gender-specific comments, or any content that can reasonably offend someone on the basis of sex, race, color, religion, national origin, age, sexual orientation, gender identity, mental or physical disability, veteran status or any protected status of an individual or that individual's relatives or associates. Any content that may be interpreted as libelous, defamatory or slanderous is prohibited.
- City Internet access shall not be used to conduct personal business, play computer games, gamble, run a business, conduct political campaigns, for personal gain, or to take part in any prohibited or illegal activity.
- No employee may use City Internet access to post a message to an Internet message board, chat room, "weblog," "listserv," or other Internet communication facility, except in the conduct of official business or support of the City's mission. The message must clearly identify the author as a City employee, by name, with the employee's official return City e-mail address or other contact information. Any opinions expressed must include a disclaimer stating that the opinions are those of the author and not necessarily those of the City of Albuquerque.
- Nothing in this policy shall be construed as requiring the City to provide any technical resources or assistance in support of any Internet use which is not directly related to the conduct of official City business.
- No employee may use City facilities knowingly to download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.
- No employee may use City facilities to monitor use of City computing or network resources by any other individual, or perform any probing, scanning, "sniffing," or vulnerability testing, except as otherwise provided by City policies or law.
- No employee may use the City's Internet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- No employee may install, remove, or otherwise modify any hardware or software for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security measures the City may have in place, except as otherwise provided by City policies.
- Employees shall not assume that any data or databases are automatically subject to public inspection under the New Mexico Inspection of Public Records Act. There are numerous exclusions to this law, and such data

may not be forwarded, uploaded, or otherwise transmitted to non-City entities without appropriate approvals.
- Infractions of these policies constitute misuse of City assets and therefore are considered violations of the City of Albuquerque Employee Code of Conduct and may result in disciplinary actions sanctioned under relevant provisions of the City Personnel Rules and Regulations.

3. RATIONALE

The City of Albuquerque provides employees access to the vast information resources of the Internet with the intention of increasing productivity. While Internet access has the potential to help you do your job faster or smarter, there is justifiable concern that it can also be misused. Such misuse can waste time and potentially violate laws, ordinances, or other City policies. This Internet usage policy is designed to help you understand the expectations for the use of these resources.

Also refer to:

- Administrative Instruction 1-7, "Inspection of Public Records Act Regulations," May 7, 2002.
- Administrative Instruction 6-5, "Use of City Property," September 1, 1992.
- Personnel Rules and Regulations Section 301.3, "Standards of Conduct."
- Personnel Rules and Regulations Section 301.12, "City Property."
- Personnel Rules and Regulations Section 301.15, "Automated Systems."

IT POLICY – INFORMATION TECHNOLOGY PROTECTION

1. SCOPE

Applies to all City information technology assets.

2. POLICY

Policy Definitions:

- **Confidentiality** – Confidentiality refers to limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people."
- **Integrity** - Integrity refers to the trustworthiness of information resources.
- **Availability** - Availability refers to the availability of information resources. An information system that is not available when you need it is almost as bad as none at all.

Policy Provisions

It is the policy of the City of Albuquerque to protect the Confidentiality, Integrity and Availability of data and, protect against disruption of the operation of its information technology assets and thereby help to protect the citizens, economy, essential human and government services, and public safety of the City.

Information must be protected according to its sensitivity, criticality and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. Maintaining the computer patch management and operating system security updates on all networked resources to include personal computers, mobile devices, application servers, printing devices and networked devices are critical in the protection of the City resources.

To ensure that City business objectives are met and the confidence of our citizens, customers, taxpayers, ratepayers and bondholders is maintained, all employees have a responsibility to protect information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional.

To ensure that City business objectives are met and the confidence of our citizens, customers, taxpayers, ratepayers and bondholders is maintained, all employees have a responsibility to protect information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional.

Except as otherwise provided by City policy:

- Protection of centrally-managed or “City-wide” information technology assets is the responsibility of the Chief Information Officer, Information Security Office or designee.
- protection of information technology assets under the physical control of a Department is the responsibility of the Department Director;
- Patch Management and Security Updates:
- The City of Albuquerque Department of Technology and Innovation (DTI) shall maintain and manage all operating system patches and security updates on personal computers, application servers, printing and all network related devices. System operating patches and security updates shall be reviewed on a monthly basis. Implementation of system operating patches and security updates shall be performed on an “as needed” basis but no longer than quarterly. All changes shall be presented to the Change Advisory Board for review.
- In all cases, protection shall be provided in compliance with all City information technology policies, standards, procedures and guidelines.

3. RATIONALE

Information technology protection requires continuous efforts to secure the information systems for critical infrastructure, including emergency preparedness communications, and physical assets that support such systems. Protection of these systems and the data which resides on systems is essential to consistent and effective service delivery.

ENFORCEMENT MEASURES FOR RESPONSIBLE AI USE

The working group recommends establishing an Emerging Technologies Board to oversee the implementation of AI and other emerging technologies across city departments. This Board would review major technology decisions, enforce policy compliance, and investigate violations, ensuring that privacy rights and equitable outcomes are upheld throughout the AI lifecycle. Acting as both a regulatory body and a bridge between city operations and the community, the Board's responsibilities would include interdepartmental coordination, stakeholder engagement, policy enforcement, and complaint resolution to maintain transparency and democratic accountability in the city's use of emerging technologies.

This Board would review major technology decisions, enforce policy compliance, and investigate violations, ensuring that privacy rights and equitable outcomes are upheld throughout the AI lifecycle.

SUGGESTED EMERGING TECHNOLOGIES BOARD RESPONSIBILITIES

- Guide and review all significant emerging technology decisions.
- Foster collaboration across departments to address technological impacts.
- Ensure public commons, privacy rights, and equitable outcomes are protected.
- Regularly engage community stakeholders to gather input and address concerns.
- Review, update, and enforce policies related to AI and emerging technologies.
- Hear complaints regarding violations of AI or emerging technology policies.
- Ensure that all major purchases and uses of AI or emerging technologies are presented to the Board.