4.30q City Use of Artificial Intelligence (AI) Regulation

Regulation Owner(s)

Organizational Effectiveness Department – Performance Analytics and Information Technology Department – Data & GIS

Legal References

Idaho Public Records Act (Idaho Code § 74-101 et seq); applicable federal and state laws governing privacy, civil rights, nondiscrimination, employment, criminal justice information, and financial data (for example, HIPAA, CJIS, and PCI-DSS, where applicable); Technology Procurement Regulation (B 8.04e); Technology, Print and Digitization Procurement Procedure; Information Security Regulation (4.30p); Data Protection and Classification Standard; city records management guidance.

Currently, Idaho has no statute governing municipalities' use of AI systems, and there is no broad federal law that applies to local governments. However, the Idaho Public Records Act (Idaho Code § 74-101 et seq.) applies to all city records, including those created, assisted, or influenced by AI systems. This means that AI-generated content may constitute a public record and is subject to disclosure and retention requirements. In this absence of broader regulation, the City of Boise has established a locally tailored set of rules, processes, and guidelines to ensure AI is used safely, ethically, and effectively in serving the community.

Purpose

This Regulation establishes binding rules for the responsible, safe, and ethical use of Artificial Intelligence (AI), including Machine Learning (ML) and Generative AI, in city operations. The intent is to harness AI to enhance public services, improve efficiency, and drive innovation, while ensuring that its deployment protects safety, preserves data integrity, and upholds transparency, accountability, and privacy.

Statement

The City of Boise will use AI to improve efficiency and deliver high-quality services. Efficiency, however, should not come at the expense of safety, protection of city and resident data, or public transparency. All AI use must uphold accountability and community trust.

Scope

This Regulation applies to all city employees, contractors, interns, volunteers, and vendors acting on behalf of the city and using AI for city related work. It sets the rules for when and how Artificial Intelligence (AI), including Generative AI and Machine Learning (ML) systems, may be used in city work, including expectations for risk review, transparency, data protection, and human oversight. It applies whenever the city is considering acquiring, configuring, or using AI-enabled tools. The detailed steps for purchasing and contracting technology are governed by the Technology, Print and Digitization Procurement Regulation (B 8.04e), and Technology Procurement Procedure.

Definitions

- **Internal City Users**: City employees, contractors, interns, volunteers, and service vendors acting on behalf of the city. Where service vendors operate AI systems on behalf of the city, their contracts must require compliance with this Regulation. This does not include the third-party AI product vendors from whom the city licenses AI tools or platforms.
- **Artificial Intelligence (AI):** A machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments.
- **AI System**: Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.
- **Generative AI**: An AI system that can generate new or significantly transformed content (such as text, images, audio, video, or code) in response to prompts or other inputs, in a way that resembles human-created content.
- **Machine Learning (ML)**: An AI approach that uses data to train models that make predictions, classifications, or decisions.
- **Prompt**: any input submitted by a user into a generative AI tool (such as text, files, or examples) to produce an output.

- **Non-Containerized or Public AI Tool:** An AI platform or service that is publicly available over the internet and is **not** configured, licensed, or controlled by the city as a Non-Containerized or Public AI Tool. Public AI Tools include consumer, personal, or enterprise accounts where the provider controls the environment and may use customer data to improve its services, and where the city cannot ensure separation of city data, retention, and audit in accordance with this Regulation.
- **Containerized or Private AI Tool**: An AI platform that is licensed, managed, and secured by the city, with technical controls that separate city use from the public version of the tool. Containerized or Private tools ensure that city data is not shared with or used to train external models, and that prompts, outputs, and related activity can be retained, audited, and disclosed in compliance with the Idaho Public Records Act and city records retention schedules.
- **Restricted or Private Data:** Refers to information classified as such under the city's Data Protection and Classification Standard, including but not limited to personally identifiable information (PII), protected health information (PHI), criminal justice information (CJI), payment card data (PCI), sensitive HR information, and critical infrastructure information.
- **Substantially Impact**: For purposes of this Regulation, "Substantially Impact" means that an AI-enabled decision or recommendation that can:
    - Approve, deny, or meaningfully change a person's or group's access to city services, permits, benefits, funding, or enforcement actions;
    - Affect an individual's employment status, pay, promotion opportunities, or discipline; or
    - Restrict rights or access to city facilities, programs, or other opportunities provided by the city.

Risk Categories for AI Use

To support consistent, risk-based governance, the city classifies AI uses into risk categories. These categories determine the level of review, safeguards, and ongoing monitoring required.

Low-Risk AI Use

Low-risk AI use means using an AI system for internal, non-sensitive tasks where:

- Outputs are reviewed and edited by city staff before being relied upon;
- The AI system does not independently approve, deny, or meaningfully change any person's access to city services, benefits, employment, funding, or legal status; and

- Internal City Users input into the AI systems only Shared or de-identified data, consistent with city privacy and security policies.

Examples include: drafting or editing internal memos, summarizing non-confidential reports, generating talking points, or formatting code for internal use.

Medium-Risk AI Use

Medium-Risk AI use includes AI uses that do not clearly meet the criteria for Low-Risk or High-Risk. Medium-Risk uses typically involve some impact on services or use of non-public data but do not independently approve, deny, or significantly change access to services, benefits, employment, or enforcement.

High-Risk AI Use

High-risk AI use means using an AI system in a way that can substantially impact individuals or communities, including when the system:

- Is used to approve, deny, prioritize, or significantly change access to city services, permits, benefits, funding, enforcement actions, or legal outcomes.
- Is used to make or support employment-related decisions, such as hiring, promotion, discipline, or termination;
- Processes Restricted or Private Data (as defined in this Regulation and classified under the city's Data Protection and Classification Standard) in a way that creates material privacy, bias, or safety risks;
- Performs automated decision-making with limited or no meaningful human review.

High-risk AI uses require additional review and safeguards as described in the Artificial Intelligence (AI) Systems Use and Governance Procedure.

When in Doubt

When Internal City Users are unsure whether an AI use is low- or high-risk, they treat it as at least Medium- or High-risk and consult their Department AI Liaison, OE, or IT for guidance.

Responsibilities

- **Organizational Effectiveness (OE) Department**: Facilitates city AI pilots, helps establish and prioritize organizational use cases, and collaborates with IT to evaluate AI systems for city use. Through the OE Performance Analytics team, advises on Medium- and High-Risk AI use cases, including both Generative AI and

ML, and provides risk advisories and recommendations. Supports training, guidance, and organizational change to help departments use AI responsibly.

- **Information Technology (IT) Department**: Reviews and advises on AI systems, maintains the city's list of city-approved solutions, and ensures security and compliance. May include AI systems in information security and compliance reviews where appropriate. Partners with OE and, where appropriate, the Data and AI Working Group to assess Medium- and High-Risk AI use cases and systems and provides technical risk and feasibility recommendations.
- **Finance Department – Procurement**: Ensures vendors disclose AI capabilities in solicitations and that procurement of AI-enabled systems follows the Technology Procurement Regulation and Technology Procurement Procedure, including required AI-related documentation and appropriate privacy, security, and ethical AI requirements in contracts. Works with OE and IT to ensure procurement decisions align with city standards.
- **Legal Department – Privacy Officer**: Ensures AI use complies with applicable laws, public records requirements, and privacy protections. Reviews high-risk use cases, advises on legal and ethical risks, and supports contract language to safeguard city and resident data.
- **Departments**: Designate an AI liaison, coordinate with OE and IT on proposed use cases, and comply with all requirements of this regulation. Ensure contractors and vendors who use AI on behalf of the city comply with this Regulation and related standards.
- **Internal City Users**: Normally use city-approved AI systems for city work, follow all rules in this Regulation, fact-check outputs, and avoid prohibited uses. Internal City Users may use personal or public AI tools only for low-risk, non-sensitive city work in line with this Regulation and the AI Systems Use and Governance Procedure (for example, no Restricted or Private Data and any applicable departmental guidance is followed).
- **Vendors/Contractors**: Disclose AI functionality, provide required AI-related documentation, and comply with city contractual standards for privacy, security, and ethical use when providing products or services to the city.
- **Data and AI Working Group:** Serves as the city's cross-departmental advisory group for data protection and AI use. For AI topics, it supports responsible AI adoption across the city; reviews selected Medium- and High-Risk AI use cases when requested by OE, IT, or departments; provides a citywide perspective on resident and internal city user impacts, equity, and community expectations; and

recommends updates to data and AI training, guidance, and standards. Only members relevant to a given use case need to participate in that review.

Rules

Approval & Procurement

- AI systems used for ongoing city work, Medium- or High-Risk uses, or that process Restricted or Private Data must be reviewed with OE and IT before use.
- Departments may not procure or deploy AI systems independently outside the Technology, Print and Digitization Procurement Regulation and Technology Procurement Procedure.
- Incidental, low-risk use of public AI tools by Internal City Users is permitted only as described in this Regulation and the AI Systems Use and Governance Procedure.
- Vendors must disclose any AI uses involving city data and provide AI-related documentation as required by the Technology, Print and Digitization Procurement Regulation and Technology Procurement Procedure.

Data Protection

- **Restricted or Private data must never be input into public AI tools**.
- All AI contracts must include data security, privacy protections, and clear ownership of city data.

Account Separation and Use of AI Tools

Public or Non-Containerized/Non-Private AI Tools

- Do not enter city confidential, regulated, or personally identifiable information (PII).
- Use is limited to low-risk, non-sensitive tasks, such as:
    - Drafting or brainstorming non-binding ideas
    - Generating background research or summaries from public information
    - Producing generic text, images, or concepts for discussion
    - Low-risk tasks do **not** include legal, financial, personnel, or constituent-specific information, or anything that could create or modify an official city record without proper review and retention.
- Internal city user who uses non-containerized/non-private tools for city business must self-disclose their prompts and outputs upon request in the event of public records request, per records management guidance.

City-Approved Containerized/Private AI Tools

- Internal City Users may use containerized AI platforms licensed and managed by the city for a broader range of work tasks.
- Use must occur only under IT-provisioned accounts.

Records & Retention

- AI user prompts and AI-generated or AI-assisted content created, received, or used in the course of city business may be considered a public record. Internal City Users must retain AI prompts and outputs consistent with existing records management guidance.
- Use of Private AI tools that cannot support retention, export, or audit must be pre-approved by IT and OE with a compliance plan in place.

Human Oversight

- AI-generated outputs must be reviewed, fact-checked, and edited by an Internal City User before being used in communications, decisions, or public records. Accountability for final content rests solely with the human reviewer.
- The depth of review should be proportionate to the risk of the use: low-risk uses (such as drafting internal memos) may require routine editing and sense-checking, while Medium- and High-Risk uses require more thorough validation and documentation as described in the Artificial Intelligence (AI) Systems Use and Governance Procedure.

Transparency & AI Disclosure

The city values transparency and public trust. When city staff use Generative AI, staff should use professional judgment about whether and how to disclose that use—especially when AI meaningfully shapes materials intended for external audiences.

Prohibited Uses

AI may NOT be used for:

- Automated decisions that **Substantially Impact** residents' or employees' rights, benefits, or access to services **without meaningful human oversight**. This includes:
    - Real-time or covert biometric identification.
    - Assigning scores or profiles to individuals that are used to grant, deny, or restrict access to services, opportunities, or benefits based on predicted behavior, personal traits, or socioeconomic status.

    - Performing individual-level emotion or sentiment analysis, or otherwise infer a person's emotional state, for the purpose of making or influencing decisions about that individual, manipulating their behavior, or targeting them for differential treatment.
    - Social scoring or classification of individuals based on personal traits, behavior, or socioeconomic status, including systems that generate generalized "risk" or "trustworthiness" scores about individuals.
- Any use that violates state or federal law, public records requirements, or exposes the city to undue risk.

NOTE: Aggregate Analytics and Planning: The prohibitions in subsections (c) through (e) do NOT prevent the city from using AI for aggregate or de-identified analytics where all of the following are true:

- Data is de-identified or aggregated such that individual people cannot reasonably be re-identified.
- Results are used to understand overall trends and improve services or workforce planning, not to take adverse action against specific individuals; and
- The analysis complies with applicable privacy, HR, labor, and records policies.

Logging and Reporting

- **System Logging and Records**: IT and system owners are responsible for enabling appropriate logging on AI systems, consistent with city information security standards (for example, access logs and basic usage metrics). Internal City Users are not required to log every individual AI prompt or interaction solely for this Regulation. However, as described in Section 4 (Records & Retention), AI prompts and outputs that document city business or are incorporated into work products must be retained in city systems of record in accordance with city retention schedules.
- **Reporting Novel or High-Risk Uses**: Internal City Users who are considering a new AI system or a new way of using an existing AI system that may be novel or High-Risk will notify their Department AI Liaison. The Department AI Liaison is responsible for coordinating with OE and IT to submit the proposal for review before deployment, using the risk and solution assessment process described in the Artificial Intelligence (AI) Systems Use and Governance Procedure. For Medium- and High-Risk proposals, this review may include OE Performance Analytics, IT Business Relationship Managers (BRMs), IT Technology Owners, and, where appropriate, the Data and AI Working Group. When Internal City Users are unsure whether a

proposed use is novel or High-Risk, they must treat it as at least Medium-Risk and seek guidance from their Department AI Liaison, OE, or IT before proceeding.

Sunset/Decommissioning

- AI systems that no longer provide benefit, fail to meet standards, or pose unacceptable risks will be phased out in coordination with IT and OE.
- Transition plans must address data ownership, records retention, portability, and service continuity.

Audit & Compliance

- IT may include AI systems and practices in existing information security and compliance reviews, in coordination with system owners. OE supports these efforts with guidance and subject-matter expertise as needed.
- Internal Audit may independently review AI governance and compliance based on Council direction.

Enforcement

Violations of this Regulation, including deploying AI systems outside the approval process, may result in:

- Suspension or removal of access to the AI system;
- Termination of the unapproved contract or system; and
- Appropriate corrective or disciplinary action under applicable HR policies and labor agreements.

Departments must promptly notify OE and IT if they become aware of AI systems that were procured or deployed outside of this process so they can be reviewed, remediated, or decommissioned.

Related Information

- State of Idaho ITS AI Resources
- Information Security Regulation (A4.30p)
- Personnel Files Regulation (4.45a)
- City Procurement and Records Management policies

Approval and Revision History

This document shall be reviewed **annually** and updated as necessary to reflect changes.

Version	Approval Date	Approver	Changes
1.0	12/01/2023	ISD	Original release
2.0	01/26/2026	Policy Committee	Replaces the city's prior AI Regulation (4.30q, 2023). The former policy focused on generative AI and four usage rules. This update expands to all AI systems, introduces risk-based review, prohibits certain high-risk uses, and integrates with the Technology Procurement Regulation (B 8.04e). It also clarifies roles for IT, OE, Legal, and the Clerk, and aligns with the city's Information Security Regulation (4.30p), Data Protection and Classification Standard, and public records requirements.

Approved By Policy Committee on 1/26/26