TOOLKIT - INSTRUMENT 3

AI Procurement Checklist

Most municipal AI arrives through vendor products, contract renewals, software updates, and pilots. Use this checklist for new purchases, pilots, renewals, amendments, and vendor-added AI features.

Vendor disclosure questions

Require written responses before approval. If a vendor cannot provide clear answers, that is itself relevant information for the city's review.

1. Does this product use AI, machine learning, generative AI, automated prediction, ranking, or decision-making in any feature? List each feature.
2. What data does the system collect, receive, generate, infer, or retain? Is any city or resident data used to train, fine-tune, evaluate, or improve vendor models?
3. Can the vendor or a third-party model provider change system behavior after contract signing? What advance notice, documentation, testing, and city approval are provided?
4. What are the known error rates, limitations, performance boundaries, and failure modes of each AI-enabled feature?
5. Has the system been evaluated for performance differences or disparate impacts across relevant demographic or affected groups? Provide available methodology and results.
6. What logs, documentation, version information, testing access, audit rights, or explanations can the city obtain for consequential outputs?
7. Where is data processed and stored? Which subcontractors, cloud providers, model developers, or third-party services are involved?
8. What happens to city data, derived data, prompts, outputs, embeddings, logs, and system configurations at contract termination?

Apply the full checklist to Tier 3 and Tier 4 systems. For lower-risk tools, prioritize the questions most relevant to data protection, security, public records, system changes, performance, and vendor accountability.

Core contract clauses

Clause	Purpose
Data reuse restriction	The vendor may not use city or resident data to train, fine-tune, evaluate, or improve models for unrelated purposes or other customers without written city authorization.
Change notification	The vendor must provide advance notice of material changes to AI features, model providers, system behavior, data practices, or performance, and allow the city to re-review the system.
Audit and logging	The city receives logs and documentation sufficient to review relevant inputs, system version, settings, human actions, and operational history associated with consequential outputs.

Clause	Purpose
Records compliance	The vendor must support the city's applicable records-retention, disclosure, litigation-hold, and public-records obligations.
Incident reporting	The vendor must report material security incidents, harmful outputs, significant performance failures, or materially incorrect results within a defined period.
Performance and acceptance testing	The city may test the system before full deployment and reject, suspend, or require remediation if agreed performance, accessibility, security, accuracy, or reliability standards are not met.
Suspension and termination rights	The city may suspend or terminate use when the system causes material harm, fails required testing, changes substantially, creates unaddressed legal or security risk, or no longer complies with city policy.
Exit and portability	City data must be returned or securely destroyed at termination, with written certification and reasonable support for migration to another system.

Review checkpoints

- Confirm the system is recorded in the AI use inventory and has an assigned risk tier.
- Confirm legal, privacy, security, records, and accessibility review for Tier 3 and Tier 4 systems.
- Name the official accountable for human review of consequential outputs.
- Confirm disclosure to residents where they interact with the system directly.
- Set a re-review date tied to contract renewal.

This template is provided for general informational purposes only and is not legal advice. Each local government should review and adapt it with its own attorney, records officer, privacy, security, and procurement staff.