publicsafetyadvisorypartners.com
561-299-0601

AI Governance Checklist

Governing Artificial Intelligence in Public Safety

Excerpted from *Executive Oversight: The City Manager's Guide to the Business of Public Safety* by Jeff Cirminiello — Chapter 11

ORGANIZATION	REVIEWED BY	DATE

PURPOSE

This checklist helps city managers and chief executives review how artificial intelligence is being used in public safety operations. The focus is on executive oversight, data control, accuracy, human review, vendor accountability, and public trust.

It is intended to support governance discussions and should be reviewed periodically. It does not replace local policy, legal counsel, procurement review, or technical standards.

1. Executive Oversight

- ☐ Leadership knows where AI is being used across public safety operations.
- ☐ Leadership understands what work, records, reports, or decisions AI may influence.
- ☐ Responsibility for AI oversight is clearly assigned.
- ☐ AI use is reviewed as an executive governance issue, not only a technology issue.

2. Data Control and Security

- ☐ Sensitive public safety information remains within approved systems.
- ☐ Leadership understands what data AI systems can access, retain, or transmit.
- ☐ Data storage, access, retention, and audit controls are clearly defined.
- ☐ CJIS, medical, investigative, personnel, and protected information are handled under existing security standards.

3. Accuracy and Human Review

- ☐ AI-generated content is reviewed by a person before it is used or finalized.
- ☐ Employees remain accountable for the accuracy of their work product.
- ☐ AI-assisted reports remain editable and subject to normal supervisory review.
- ☐ Systems cannot finalize or submit official reports without meaningful human review.

4. Operational Visibility

- ☐ Leadership understands what the AI tool does and how it supports the workflow.
- ☐ AI systems are reviewed for accuracy, consistency, and operational impact.
- ☐ The organization has a process for identifying errors, limitations, or unintended results.
- ☐ Leadership receives enough information to know how AI is affecting operations.

© 2026 Public Safety Advisory Partners. May be reproduced for internal governance use.

5. Policy, Training, and Informal Use

- ☐ Policies define approved and prohibited AI use.
- ☐ Employees are trained on informal or unauthorized AI use.
- ☐ Employees know what information may not be entered into open AI systems.
- ☐ Employees know who to ask when they are unsure whether a use is allowed.

6. Vendor and Procurement Oversight

- ☐ Vendors disclose whether AI is included in the product or platform.
- ☐ Leadership understands where AI-related data is stored and processed.
- ☐ Procurement reviews include data control, accuracy, human review, and accountability.
- ☐ Vendor tools do not set operational policy by default.

7. Public Trust and Communication Readiness

- ☐ Leadership can explain why the AI tool is being used.
- ☐ Leadership can explain the safeguards, limitations, and human review process.
- ☐ Leadership understands how AI errors or misuse could affect public trust.
- ☐ Communication expectations are established before an incident or controversy occurs.

Executive Framing Statement

Public safety organizations do not need to avoid artificial intelligence. They need to govern it with clear rules, controlled data, human review, and leadership accountability.

© 2026 Public Safety Advisory Partners. May be reproduced for internal governance use.