# CRCOG Municipal AI Use and Security Policy

Important Disclaimer: This template is intended to assist organizations in drafting an initial outline for an AI policy. It is not legal advice and does not create an attorney-client relationship. The resulting draft should be reviewed by a qualified attorney or legal professional to ensure compliance with applicable laws, regulations, and organizational requirements.

Important prerequisite- If your municipality does not have an operational Acceptable Use Program (AUP), do not proceed with this AI policy. This policy requires integration into the overall Acceptable Use Program. AI is another form of technology that needs to be governed by the overall information system's AUP.

Municipal Government AI Use and Security Policy

Effective Date: [Insert Date]
Approved by: [Insert Authority]
Policy Owner: [Insert Department, e.g. Town Manager's Office]

## 1. Purpose

This policy establishes guidelines for the secure, ethical, and responsible use of artificial intelligence (AI) systems across all departments within the [municipality]. It aims to protect data, uphold public trust, and comply with applicable laws and ethical standards.

## 2. Scope

This policy applies to all employees, contractors, consultants, volunteers, and third-party entities who use, manage, or develop AI systems on behalf of the municipality.

## 3. Definitions

**Artificial Intelligence (AI):** Systems or applications that perform tasks typically requiring human intelligence, including but not limited to natural language processing, machine learning, computer vision, and decision-making algorithms.

**High-risk AI:** AI systems that significantly impact public services, data privacy, or public safety, including systems used for law enforcement, eligibility decisions, critical infrastructure, or surveillance.

**AI Tool Register:** A record of all approved AI systems used by the municipality.

**AI Risk Assessment:** A structured evaluation of the risks associated with implementing or using an AI system.

**Closed Systems:** AI Systems where data and information are not publicly available.

**Open Systems:** AI Systems where data, models, and information are accessible by public viewers.

## 4. Policy Statements

### 4.1 Governance and Oversight

The IT Department, in collaboration with the [Insert appropriate town departments], shall establish an AI Governance Committee responsible for approving high-risk AI systems and overseeing compliance.

Each department must designate an AI Liaison to ensure local compliance with this policy and to coordinate risk assessments.

All use of AI must comply with local, state, and federal policies, laws, and regulations (State of CT AI Policy and Guidelines).

### 4.2 AI Tool Approval

All AI tools must be reviewed and approved before implementation. Departments must submit a request using the AI Risk Assessment Template (Appendix A).
Approved tools shall be documented in the AI Tool Register (Appendix B).
Unapproved or unauthorized AI tools (including AI browser extensions, plugins, or unverified SaaS platforms) are prohibited on municipal devices and networks.

### 4.3 Risk Management

Prior to implementation, departments must conduct an AI Risk Assessment addressing:
- Data sensitivity and protection requirements
- Impact on residents and municipal operations
- Bias and discrimination risks
- Transparency and explainability
- Security and privacy safeguards

High-risk AI systems require approval by the AI Governance Committee and may trigger additional requirements such as public consultation or third-party audits.

### 4.4 Data Protection and Privacy

AI systems must comply with municipal data protection policies, including limitations on the use of personal information.

Any use of AI involving identifiable personal data must implement data minimization, encryption, and access controls.

Systems using biometric data (e.g., facial recognition) are prohibited unless authorized by municipal ordinance and subject to specific safeguards.

### 4.5 Transparency and Accountability

When AI is used to make decisions affecting individuals (e.g., eligibility for services), the system must be auditable, and a human-in-the-loop must be available to review and override decisions.

Departments must maintain documentation of how the AI system operates, including training data, logic, and outputs, where feasible.

Departments are responsible for monitoring AI system performance and updating models or configurations to prevent degradation or unintended impacts.

Departments are responsible for reviewing anything produced by AI for accuracy (e.g., meeting minutes, etc.)

### 4.6 Training and Awareness

Employees must complete annual training on AI use, risks, and compliance.
Department heads are responsible for ensuring their teams understand and follow this policy.

### 4.7 Incident Response and Reporting

AI-related incidents, including data breaches, unauthorized use, or system errors impacting services, must be reported immediately to the IT Security Office.
An AI-specific incident response plan shall be developed and integrated into the municipality's broader cybersecurity incident response plan.

### 4.8 Data Retention and E-Discovery

- Implement data retention policies complying with laws and regulations.
- Store AI data securely, including training data, operational data, and decision logs.

- Define retention periods and securely dispose of expired data.
- Prepare for e-discovery, ensuring access to relevant AI data and documentation.
- Design systems to facilitate extraction and review of AI-related data.
- Conduct regular audits for compliance and effectiveness of e-discovery procedures.

## 5. Enforcement

Violations of this policy may result in disciplinary action, including revocation of access, reassignment, or legal action, depending on the severity and intent of the violation.

## 6. Review and Updates

This policy shall be reviewed at least annually or upon significant changes in AI technology or regulatory requirements.

## Appendix A: AI Risk Assessment Template

1. System Overview: What is the purpose of the AI system? Who are the vendors or developers?
2. Data Inputs: What data is used? Does it include personal or sensitive data? How is data collected and stored?
3. Risks to Individuals: Could the system result in discrimination, exclusion, or unfair treatment? How are biases being addressed?
4. Decision-Making Role: Is the AI making or assisting in decisions? Are there human reviewers for high-impact decisions? And, at what stages?
5. Security Controls: What security measures are in place (e.g., encryption, access control)? Has the system undergone a vulnerability assessment?
6. Monitoring and Auditing: How will the system be monitored over time? Who is responsible for oversight?
7. Legal and Ethical Compliance: Are there legal or ethical considerations (e.g., data privacy laws, anti-discrimination)?
8. Public Transparency: Will the public be notified of this system? How is transparency maintained?
9. Data Retention: What is the policy for data retention and deletion? How long is data kept before it is deleted or anonymized? Are retention policies in compliance with relevant regulations and standards?

## Appendix B: Approved AI Tool Register [NOTE: This is an example]

| Tool Name | Vendor | Department | Purpose | Risk Level | Approval Date | Expiration/Review Date |
|---|---|---|---|---|---|---|
| ChatMunicipal GPT | OpenAI | Communications | Drafting newsletters | Medium | 2024-06-12 | 2025-06-12 |
| StreetCam AI | Acme Vision | Public Works | Detect potholes from video | High | 2024-08-01 | 2025-08-01 |
| BudgetBot | FiscalSoft | Finance | Budget trend forecasting | Low | 2025-02-15 | 2026-02-15 |