AI IN ELECTIONS

Essentials for Risk Management

ELECTION OFFICIAL RISK MANAGEMENT SERIES

ELECTION SECURITY *Exchange*

This guide provides the foundation for managing AI in the election office. A proactive, structured approach—clear policies, secure tools, staff training, and strong human oversight—helps officials harness AI's benefits while mitigating risks and safeguarding election integrity.

In this guide, you will learn:

- The importance of developing an AI use policy now, and what should be in it
- The role of training in making your policies more effective
- Why you must define a clear use case before adopting any tool
- The essential differences between free and paid AI platforms
- Critical security settings to configure for any tool
- The non-negotiable rule of verifying information
- Why staying vigilant is crucial

1. You Need a Policy

Staff across the organization are likely using AI tools for work, whether or not you have a use policy in place. An absence of policy is potentially inviting more significant, unmanaged risk. A formal use policy is one of your best safety tools, providing clear guardrails to protect both the organization and individuals' rights. Microsoft assembled a template for election officials as a starting point. A few essential components are highlighted below:

Gaining Leadership Buy-in

- **When speaking with IT/security:** Frame a use policy as a safety tool. It's a mechanism to limit the misuse and sharing of sensitive information.
- **When speaking with executives:** Frame the policy as an organizational asset that enables innovation and efficiency while limiting risk and reputational damage and serving as one of the most cost-effective security controls that can be implemented

What Should Be Addressed in Policy?

- **Definitions:** Key terms like "Artificial Intelligence" and "Generative AI" should be defined to inform staff and ensure consistent application.

- **Human-centric approach and oversight:** AI systems should extend human capabilities and amplify their work, not replace people. Humans must also thoroughly review and validate any output for accuracy and appropriateness.
- **How AI can and cannot be used:** Define clear parameters around the types of data that can be used and the permissible ways they may be applied to work. This helps prevent unauthorized or inappropriate use.
- **Consequences for breaking the rules:** Clearly outline repercussions for not adhering to policy.
- **Data handling:** A critical element. Develop rules for sensitive data, what can be used, and ensure it's anonymized to maintain security and privacy.
- **Roles and responsibilities:** Establish and designate clear roles that address oversight, guidance, and enforcement of policy.
- **Transparency and disclosure:** The use of AI must be disclosed, particularly when it significantly contributes to work products, and when the public interacts with AI-enabled tools. Jurisdictions must consider public messaging as they build and refine their approach.

2. Prioritize Training

A policy only goes so far if no one reads it or understands it. Mandatory and routine training is vital to support policy enforcement and minimize risk. Valuable resources, such as **The Elections Group's Introduction to Generative AI** and **Arizona State University's Mechanics of Democracy AI + Election Clinic**, can help shape a comprehensive training program. A training program should cover:

- What is AI?
- What are the rules?
- How can it or not be used?
- What are potential risks?
- Are there approved tools?

3. Decide Why You're Using It: *Define Your Use Case*

Before diving into the deep end, take a moment to ask: What problem are we trying to solve? According to the U.S. General Services Administration AI Center of Excellence, well-defined use cases and planning can support broader alignment across the organization, including helping teams understand which problems AI-enabled tools best tackle. A good use case is specific and not ambiguous.

- **Unclear:** "We want to use AI to save time."
- **Better:** "We will use an approved AI tool to generate first drafts of public-facing voter education materials for our website and social media channels, which our staff will review, edit, and approve."

Why does this matter?

This helps identify a more appropriate tool or a series of tools to support the use case. It also helps ground acceptable uses of the selected tool, preventing staff from using it for unapproved tasks.

4. Choose the Right Tool(s)

Paid AI plans are generally safer. These plans often include agreements not to use your data for training, stronger security measures like encryption or multi-factor authentication, and access to more robust models.

Bottom line: For any official election work, it's recommended to use a paid version where you have a guarantee that your data remains in your control.

5. Lock It Down

Regardless of which tool you use, it's important to review the settings, as with any other election application. Safeguards and security best practices can go a long way in mitigating risk and ensuring AI tools are helpful, as noted by the Brennan Center for Justice.

- **Turn off Data Sharing:** This is a critical setting. Locate your account and privacy settings and opt out of any data sharing used for "model improvement" or "training". If this is unavailable, you should not use it for work.
- **Enable 2-Step Login (MFA):** Like any other account, this provides an essential layer of security. It ensures that a compromised password alone is not enough to grant an attacker access.
- **Know Who's Using It:** Maintain strict controls over who has access to the tool, especially if you're using it as a team. Remove former employees immediately and ensure current staff have access only to the tools they absolutely need to do their jobs (principle of least privilege).

6. Verify, Verify, Verify: *You're in Charge*

AI can make mistakes. It can "hallucinate," which means it may generate false information, including fabricating information that may look legitimate on the surface, but it's actually not true. A human must check the work, especially before anything is made publicly available.

7. Stay Informed and Adapt

The landscape is rapidly evolving. New tools, capabilities, and use cases are constantly emerging, as are threats. Election officials must pay attention to understand how AI can impact their work or stay informed about vulnerabilities, a key aspect of risk management. Specialized resources, such as the ASU AI & Elections Clinic's Substack, are a practical way to keep pace with developments and capabilities.

Further Resources and Templates

Additional resources and templates are provided below to supplement the information in this document. This is not an exhaustive list, but it provides a helpful starting point. Election officials should review these resources and share them with key partners to prepare for AI adoption and mitigate associated risks.

Simple and Quick

- ASU AI & Elections Clinic Substack
- GovAI Templates
- Microsoft AI Use Policy for Election Officials Template
- Microsoft Election Prompt Library
- Microsoft Intro to Gen AI for Election Officials
- NACo AI and GenAI in Motion
- Regional Government Services AI Resources for Local Gov
- The Elections Group AI Cookbook

Technical and Detailed

- GSA AI Guide for Government
- NIST AI Risk Management Framework (1.0)
- NIST AI Playbook
- OWASP AI Exchange
- AI and Election Security Committee Final Report
- Preparing for AI & Other Challenges to Election Administration | Bipartisan Policy Center