MULTISTATE TAX COMMISSION

444 North Capitol St., NW
Suite 425
Washington, DC 20001-1538
Telephone: 202.650.0300

www.mtc.gov

Artificial Intelligence (AI) Use Policy

Effective Date: [Insert Date] | Approved By: Keith J. Richardson, Executive Director | Review Cycle: Semi-Annual

1. Purpose

This policy establishes standards and guardrails for the use of artificial intelligence (AI) tools by employees, interns, contractors, and representatives (collectively referred to as "staff") of the Multistate Tax Commission ("MTC" or the "Commission"). It is intended to enable staff to benefit from AI-assisted productivity while protecting the confidentiality of member-state tax information, the integrity of the MTC's analysis and publications, and the Commission's reputation as a trusted intergovernmental body.

2. Scope

This policy applies to all MTC staff, and to all AI tools used in connection with MTC business. It applies regardless of whether the tool is Commission-provided or independently accessed by staff.

3. Definitions

- "AI tool" – any software, feature, or system that uses artificial intelligence to generate, analyze, summarize, classify, predict, recommend, or otherwise process information, or to perform or initiate actions on a user's behalf. AI tools include, but are not limited to, generative AI chatbots, AI writing or coding assistants, AI-powered transcription tools, AI features embedded in existing software (e.g., document, spreadsheet, or research platforms), AI-based data analysis tools, AI search tools, agentic AI tools, and other similar technologies.
- "Confidential information" – information protected under state confidentiality statutes governing tax administration, non-public taxpayer data, draft audit or litigation positions, internal deliberations, personnel data, and any other information that is confidential by law or designated by the Commission as confidential.
- "Approved AI tool" – an AI tool that has been reviewed and authorized for use by MTC's IT function under Section 9. AI tools using information classified as confidential information must also be approved by legal counsel.

4. Guiding Principles

1. Confidentiality first. Member-state tax information and taxpayer data should never be entered into an AI tool unless that tool has been specifically approved for that purpose and appropriate data-handling agreements are in place.
2. Human accountability. AI may assist staff, but staff — not the AI tool — remain responsible for the accuracy, appropriateness, and professional judgment reflected in any work product.
3. Proportionate risk management. Higher-risk uses (e.g., anything touching taxpayer or member-state confidential data) require stronger controls than low-risk uses (e.g., drafting a generic internal memo outline).

5. Permitted Uses

Subject to the restrictions in Section 6, the confidentiality requirements in Section 7, and all other requirements in this AI Use Policy, staff may use approved AI tools for activities such as:

- Drafting or editing internal memos, training materials, agendas, minutes, invoices, policies, presentation slides, and general correspondence that do not contain confidential information.
- Summarizing publicly available materials, such as published state statutes, regulations, court decisions, or other organizations' public reports.
- Brainstorming outlines, meeting talking points, or training materials.
- Generating or debugging code for internal tools, using synthetic or already-public sample data.
- Improving the clarity, tone, or grammar of documents that do not contain confidential information.
- Research assistance that is treated as a starting point requiring independent verification, not a final source.

6. Prohibited and Restricted Uses

6.1 Prohibited without exception

- Entering confidential information into any AI tool that has not been specifically approved for that purpose with appropriate contractual data protections.
- Using output from an AI tool as the sole basis for a legal, policy, or audit-related conclusion without professional review and verification.
- Using any AI tool that can autonomously take or initiate actions, access MTC information or systems, communicate externally, or otherwise act on the MTC’s behalf.

6.2 Requires prior approval from IT

- Connecting any AI tool to MTC email, shared drives, case management systems, or other internal systems via plugins, browser extensions, or API integrations.
- Using AI vendors' “enterprise” or “business” tiers where a data processing agreement has not yet been executed.

Any staff member that engages in a prohibited or restricted use without approval from IT is subject to disciplinary action as described in the compliance and enforcement provisions in Section 11.

7. Data Handling and Confidentiality

Before using any AI tool, staff must classify the information involved:

- Public – already published or approved for public release. May be used with approved AI tools.
- Internal, non-confidential – not yet public but not confidential information (e.g., a draft internal agenda). May be used with approved AI tools that meet the Commission's minimum data-protection standards (see Section 9.1).
- Confidential information – may only be used with an AI tool specifically approved for that data category after consultation with IT and legal counsel. AI tools for confidential information shall be subject to the minimum standards in Section 9.1 and the enhanced protection standards applicable to confidential information in Section 9.2.

When in doubt about classification, staff should treat the information as confidential and consult their supervisor or IT before using an AI tool.

8. Accuracy, Verification, and Disclosure

- AI-generated content must be independently reviewed for accuracy before use; AI tools can produce plausible-sounding but incorrect statements ("hallucinations"), including incorrect citations to statutes, cases, or figures.
- Any statutory citation, case citation, or numerical figure produced by an AI tool must be verified against the primary source before it is relied upon or published.
- Substantive use of AI in a work product intended for the Commission, member states, or the public (e.g., a report, model statute commentary, or public presentation) should be noted to the requesting supervisor or committee upon request, consistent with normal professional practice for research assistance.
- Staff should not represent AI-drafted analysis as their own independent professional judgment unless they have reviewed, verified, and taken ownership of its conclusions.

9. Approved Tools and Minimum Standards

IT maintains a list of approved AI tools, along with the data classifications each is approved for. Requests to add an AI tool should be directed to IT and must include the name of the tool and vendor, a summary explaining how the tool will be used, and a list of the types of data that will be entered into the tool.

9.1 Minimum Standards

An AI tool may be added to the approved list for information classified as internal, non-confidential or confidential information only where the vendor provides, at minimum:

- A written commitment or technical configuration ensuring that customer inputs are not used to train or improve the vendor's models (or an enterprise/API tier with that guarantee).

- Data encryption in transit and at rest.
- A defined data retention and deletion policy.

9.2 Enhanced Protection Standards for Confidential Information

An AI tool may be added to the approved list for information classified as confidential information only if it meets the minimum standards in Section 9.1, plus the following enhanced protection standards, as reviewed and approved by legal counsel:

- A signed written agreement containing appropriate confidentiality, data protection, and data use restrictions
- A contractual obligation for prompt notification in the event of a security incident or data breach involving company data
- Compliance with applicable data protection requirements

10. Training and Support

IT will provide periodic training on approved AI tools, data classification, and safe use practices. New staff will receive an overview of this policy as part of onboarding. Questions about whether a specific use is permitted should be directed to a supervisor or IT before proceeding.

11. Compliance and Enforcement

Violations of this policy, particularly the disclosure of confidential information to an unapproved AI tool, will be treated as a serious matter subject to disciplinary procedures. Any staff member who engages in a prohibited use or a restricted use under Section 6 without the required approval from IT may be subject to disciplinary action, up to and including suspension or termination of employment with the Commission. Staff who become aware of a possible violation, including an inadvertent one, must report it to their supervisor and IT as soon as practicable, but no later than 24 hours after becoming aware of it, so that any necessary remediation (e.g., contacting a vendor to request data deletion) can begin quickly.

12. Policy Review

Given the pace of change in AI technology, this policy will be reviewed at least semi-annually by IT and the Executive Director, and updated as needed to reflect new tools, risks, and member-state expectations.

13. Acknowledgment

All staff will be asked to acknowledge that they have read, understood, and agree to comply with this policy, and to renew that acknowledgment upon any material update to the policy.

_____ _____

Employee Signature Date

— End of Policy —