COMMONWEALTH of PENNSYLVANIA ARTIFICIAL INTELLIGENCE POLICY

KEY POINTS & HIGHLIGHTS
Effective January 13, 2026
Scheduled review: January 2027

01 / CORE POLICY REQUIREMENTS

Purpose & scope. The policy sets guidelines for integrating AI into Commonwealth business and decision-making. It applies to employees and contracted resources in agencies under the Governor's jurisdiction and other entities connecting to the Commonwealth Network.

Core principle: AI can support government work, but people remain responsible for oversight, verification, and decisions.

1. USE ONLY APPROVED ENTERPRISE AI TOOLS

- Only Commonwealth-approved enterprise generative AI tools may be used for Commonwealth business. Sign in with Commonwealth credentials.
- Personal use of non-enterprise AI tools with a Commonwealth email account is prohibited. Procured tools must have terms and conditions established with the Commonwealth.

2. PROTECT SENSITIVE & NON-PUBLIC INFORMATION

Never enter prohibited information into generative AI prompts, tools, or systems, including:

- Personally identifiable information (PII), protected health information (PHI), sensitive security information, or regulated data.
- Confidential, privileged, proprietary, or other non-public information; production code; or information exempt from disclosure under the Right-to-Know Law (RTKL).
- Class C data, as defined by the Commonwealth Data Classification Policy.

Assume prompts may not be private. Do not enter information you would not include in a public-facing document or email.

3. HUMAN OVERSIGHT & ACCOUNTABILITY

- Users are accountable for AI-assisted work and must review and verify every output. Reviewers need sufficient subject-matter expertise.
- AI may inform decisions but cannot make final decisions on behalf of employees. It may not make subjective or value-based judgments, including final employment decisions.
- Decisions with legal, financial, human resources, legislative, organizational, or regulatory impacts require human verification.

4. CHECK ACCURACY, BIAS & RELIABILITY

AI can produce fabricated ("hallucinated"), inaccurate, outdated, biased, inappropriate, or copyright-infringing content. Before using outputs:

- Verify facts, figures, citations, legal references, and technical claims against reliable sources.
- Check that information is current; look for stereotypes, unsupported assumptions, and inappropriate content.
- Consider copyright and intellectual-property risks. Do not rely on outputs you lack the expertise to validate.

5. DISCLOSE AI USE IN EXTERNAL CONTENT

Disclose generative AI use in public-facing or externally shared content—even if AI generated only part. Disclosure must be prominent and identify the AI system and version. Example: *"ChatGPT-3.5 was used in the creation of this document."* AI solutions interacting with customers on an agency's behalf must disclose that the customer is interacting with AI.

TURN OVER → RISK, ACCEPTABLE USE & MANAGER CHECKLIST

COMMONWEALTH of PENNSYLVANIA ARTIFICIAL INTELLIGENCE POLICY

KEY POINTS & HIGHLIGHTS
Effective January 13, 2026
Scheduled review: January 2027

02 / PRACTICAL USE & MANAGEMENT RESPONSIBILITIES

6. ASSESS RISK BEFORE USING AI

RISK / IMPACT	POLICY GUIDANCE
Low risk / high impact	Potential opportunity for productive use, with appropriate verification.
High risk / low impact	Generally avoid when the benefit is small relative to the risk.
High-risk decisions	Require additional review and governance, as applicable.

AI solutions used for certain high-risk matters—including material financial transactions, administrative policy or program changes, benefits eligibility, life-changing decisions, and health, safety, or welfare—are subject to audit requirements.

7. EXAMPLES OF ACCEPTABLE USES

When using an approved tool, public/non-confidential information, and proper review:

- Draft job postings, job descriptions, memos, and communications.
- Summarize or paraphrase text; rewrite technical information in plain language.
- Brainstorm meeting activities and discussion questions.
- Compare public policy documents and identify changes for manual verification.

These examples are illustrative, not a comprehensive list of permitted uses.

8. PROMPTING PRACTICES

- Define the task and purpose; select an appropriate tool; write a clear, specific prompt.
- Provide relevant context using permitted information and accurate data.
- Specify the audience, format, and desired level of detail.
- Review, edit, and verify the output. Better prompts do not replace human review.

9. RECORDS, GOVERNANCE & SECURITY

- Understand how the tool uses prompts and input data. Retain prompts and input data used in AI solutions for potential audits, consistent with records-management requirements.
- Before deployment, establish appropriate governance and assess data quality, bias, privacy, security, legal obligations, intellectual property, and third-party terms.
- Maintain appropriate testing, validation, documentation, audit logging, human verification, monitoring, and incident-response procedures.
- AI solutions must comply with applicable Commonwealth IT policies, privacy requirements, and other regulations.

10. EMPLOYEE & MANAGER CHECKLIST

✓ **Authorized?** Is the tool approved for this use?
✓ **Information safe?** Does the prompt contain sensitive, confidential, proprietary, or non-public information?
✓ **Risk understood?** Could an inaccurate or biased result cause harm?
✓ **Verified?** Can a qualified person check the output?
✓ **Requirements met?** Are review, approval, disclosure, or record-retention steps required?

BOTTOM LINE | Use approved tools. Protect sensitive information. Verify outputs. Disclose externally shared AI-generated content. Retain required records. Keep people accountable for decisions.

Resources: Commonwealth Artificial Intelligence Resource Center for approved tools, access instructions, and supplemental guidance on disclosure, coding, translation, transcription, and AI-assisted search.

Source: Commonwealth of Pennsylvania, Artificial Intelligence Policy, effective January 13, 2026.
https://www.pa.gov/content/dam/copapwp-pagov/en/oa/documents/policies/it-policies/artificial%20intelligence%20policy.pdf

This handout summarizes key provisions and does not replace the full policy or related guidelines.