JOINT CIRCULAR

STATE OF NEW JERSEY

NO.: 25-OIT-001	ORIGINATING AGENCIES: - OFFICE OF INFORMATION TECHNOLOGY (OIT) - OFFICE OF HOMELAND SECURITY & PREPAREDNESS, CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL (NJCCIC)	PAGE 1 OF 5
EFFECTIVE DATE: IMMEDIATE	EXPIRATION DATE: INDEFINITE	SUPERSEDES: 23-OIT-007
SUBJECT: STATE OF NEW JERSEY GUIDANCE ON RESPONSIBLE USE OF GENERATIVE AI		
ATTENTION: DIRECTORS OF ADMINISTRATION, CHIEF INFORMATION OFFICERS, AGENCY IT MANAGERS, AND AGENCY CHIEFS OF STAFF		
APPLIES TO:	FULL TIME, PART TIME AND STAFF AUGMENTATION IT/TECHNOLOGY STAFF AND BUSINESS STAFF SUPPORTING APPLICATIONS AND WEB-PRESENCE FOR STATE AGENCIES	
FOR QUESTIONS:	SEND QUESTIONS TO: CTO@TECH.NJ.GOV	

I. PURPOSE

A. Generative AI refers to a new set of technologies that use machine learning techniques to generate content in response to user input.

B. These new tools have the potential to be extraordinarily useful to public servants in their work, but they also present risks. These guidelines serve as an interim resource for employees of the State of New Jersey to help navigate the benefits and risks of these emerging technologies.

C. Generative AI is a tool, not actual intelligence. We remain responsible for the outcomes and uses of these tools.

D. As we explore the responsible use of artificial intelligence, we embrace the following principles to guide our efforts. These shared values of empowerment, inclusion, transparency, innovation, and risk management will steer our experimentation and decision-making when employing these rapidly evolving technologies.

E. With this Circular, we aim to build trust, spur progress, and ensure AI serves the public good. This Circular presents state guidelines for the use of AI. For information about enterprise AI tools and for tips and how-to's for using generative AI, please see this Frequently Asked Questions page.

II. **POLICY**

A. GENERAL

1. **Empowerment.** The use of AI should support our workforce to deliver enhanced services and products efficiently, safely, and equitably to all residents. We rely on the judgment of our professionals to ensure we realize the benefits of these tools.
2. **Inclusion and Respect.** As public stewards, we will use tools respectfully to reflect values of equity and social justice.
3. **Transparency and Accountability.** Transparency builds trust and enables collective learning. When we use AI, we must disclose responsibly and share our workflow freely with other public servants and with the public.
4. **Innovation and Risk Management**. We embrace responsible experimentation; we will maintain accountability and respect privacy and security while developing uses that drive efficiency, dialogue, and better service. We understand risks may not be fully apparent initially and commit to proactive risk assessment.

B. USE GUIDELINES

1. **Training.** Before accessing or using generative AI in their official capacity, all state employees should take the "Responsible AI for Public Professionals" course available in the New Jersey Civil Service Commission (CSC) Center for Learning and Improving Performance (CLIP) Learning Management System (LMS). The training can be accessed as a State Learner or as an External Learner.

2. **Review AI-generated content.** Verify all AI-generated content, especially for public use. Generative AI can produce clear language, but the information may be inaccurate or outdated. Watch for: incorrect facts, events, links, or references; and biased information potentially harmful to vulnerable groups like racial, ethnic, and gender minorities, people with disabilities, etc. Human review of AI content should cover the following elements:
   a. accuracy;
   b. gender, racial, and other types of bias;
   c. completeness;
   d. accessibility;
   e. and style.

   For more guidance on appropriate review methodology, please consult the FAQ page: How do I review AI-generated content before publishing?

3. **Obtain clearance for resident-facing or decisional generative AI systems and disclose their use.**
   a. *Resident-facing generative AI systems* have residents interacting directly with AI-generated content not reviewed by a human. Example: live generative AI chat bot.
   b. *Decisional generative AI systems* make decisions that impact residents directly. AI systems that produce advisory decisions that are reviewed by humans are also subject to this rule. Examples: an AI system that

evaluates applications; an AI system that recommends whether to approve an application.

c. The use of resident-facing or decisional generative AI systems **must be cleared by the State Chief Technology Officer or their delegate** and registered with the NJ Office of Information Technology (OIT).

d. When resident-facing or decisional generative AI systems are used, **disclosure of generative AI use** must be displayed prominently to the user.

e. It is recommended but not required that when residents interact directly with AI-generated content, they are provided a feedback mechanism to flag incorrect or unhelpful content, and they are directed to contact information for help. Examples: “contact us” text box, email address, feedback widget.

Sample AI-generated content disclosures:

“Chat responses were generated by a generative artificial intelligence (AI) system based on website content and reviewed by staff for accuracy.”

"This decision was made with assistance from a generative artificial intelligence (AI) system and reviewed by staff. Contact [email] for more information or to report an error.”

4. **When handling sensitive information, use a State-Approved AI Tool** (See the FAQ page: State-Approved AI Tools and Approval Process.)
    a. Sensitive Personally Identifiable Information (SPII - see Appendix A for definition) may only be used under the following conditions:
        i. The tool used is a State-Approved AI Tool such as the NJ AI Assistant (ai-assistant.nj.gov). Please see the FAQ page: State-Approved AI Tools and Approval Process for a list of approved tools and an overview of the approval process.
        ii. The tool use is approved by your Agency Chief Information Officer (CIO): The Agency CIO refers to your agency's head of information technology. The exact title and responsibilities can vary depending on the size of the organization, and how it structures its executive leadership. (For example, it could be the Agency IT Manager or IT Director). If you are unsure, ask your agency head or chief of staff.
        iii. The use of SPII must be for legitimate business purposes.

    b. **When prompting any public AI assistant, tool, or anything that is not listed as a State-Approved AI Tool, do not disclose Sensitive Personally Identifiable Information**. Any information put into public AI assistants or tools can be leaked.
        i. Do not share PII about residents, colleagues, or yourself. Do not share confidential or sensitive content. This includes names, addresses, social security numbers, other identifying numbers,

photographs, and IP addresses.

ii. Do not use AI tools to transcribe or summarize meetings where sensitive topics are discussed, including any predecisional or confidential information.

iii. Do not share any information that you wouldn't share publicly.

5. **Use appropriate tools for meeting transcription and summarization.**
   a. **Only tools approved through NJOIT and NJ Cybersecurity and Communications Integration Cell (NJCCIC) review processes may be used** for transcription and summarization when sensitive content or sensitive PII is discussed in a meeting. Approved tools are listed in the FAQ page: State-Approved AI Tools and Approval Process.
   b. When sensitive content and sensitive PII will not be discussed in a meeting, any AI transcription and summary tool may be used at the discretion of the meeting organizer. Check with the meeting organizer before activating any AI transcription and summary tools.
   c. When AI transcription and summary tools are used, their use should be disclosed clearly to all meeting participants either through a verbal announcement or a clearly visible notice in the meeting interface.

APPENDIX A: DEFINITION OF PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information and Sensitive Personally Identifiable Information are defined consistent with the Statewide Information Security Manual. The guidelines about using PII laid out in this Circular concern only *Sensitive Personally Identifiable Information (SPII)****.*** These terms are defined as follows:

Personally Identifiable Information (PII) - NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an agency, including:

1. Any information that can be used to distinguish or trace an individual‘s identity, such as name, Social Security number, date and place of birth, mother‘s maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include but are not limited to the following:

- Name, such as full name, maiden name, mother’s maiden name, or alias;
- Personal identification number, such as Social Security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number or title number and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Non-Sensitive Personally Identifiable Information (PII) - Personally identifiable information that is available in public sources, the disclosure of which cannot reasonably be expected to result in personal harm.

Sensitive Personally Identifiable Information (SPII) - Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.