Comment of Individual Maricopa County Judicial Branch Officers on Petition to Adopt Rule 135

Exhibit 2

JUDICIAL BRANCH OF ARIZONA IN MARICOPA COUNTY

Section: **CS-144** Subject: **ARTIFICIAL INTELLIGENCE GOVERNANCE POLICY** Policy ☒ Procedure ☒ Information ☒ Policy Authority **Rule 123** Public Access to the Judicial Records of the State of Arizona; **ACJA 1-509:** Use of Generative AI Technology and Large Language Models Related Documents **Security Approved AI Tools List**	Original Date: 09/08/2025 *Approved by:* **The Honorable Pamela Sue Gates** Presiding Judge

I. PURPOSE

The advancement of Artificial Intelligence within the justice system continues to expand and will impact the work of courts throughout the United States. This evolution brings opportunities to improve services to meet the growing needs of the Judicial Branch and the public we serve. It also brings new challenges and concerns that must be governed accordingly. The Judicial Branch remains unwavering in its position that judicial decision-making is a fundamentally human function-grounded in impartiality, legal expertise, empathy, and accountability. While Artificial Intelligence may serve as a valuable tool to support judicial operations, it must never supplant the human judgment essential to the fair and just administration of law.

The Artificial Intelligence Governance Policy governs the application and acceptable use of artificial intelligence tools and generated content in the Judicial Branch of Arizona in Maricopa County, hereafter called "Judicial Branch". This Policy is adopted to maintain the highest standards of security, integrity, and confidentiality while establishing required protocols and procedures for AI.

II. APPLICABILITY

The AI Security Standards outlined in this policy apply to all Judicial Branch Personnel, including Superior Court Judicial Officers and employees, Adult and Juvenile Probation employees, and other users of Branch technology resources including contract and temporary workers.

III. DEFINITIONS

A comprehensive set of terms and definitions for security policies and standards is located on the Court Technology Services' Information Security Office's SharePoint Page but for ease of reference, the following are terms used in this document.

Terms defined here are capitalized when used in this document.

Artificial Intelligence (AI) refers to the technology that enables computers and machines to simulate human intelligence, including pattern recognition, data processing, task automation, comprehension, learning,

problem-solving, decision-making, creativity, and autonomy. AI systems can perform tasks that typically require human intelligence, such as recognizing objects, understanding and responding to human language, learning from new information, and making recommendations.

AI Tool is an AI product, solution, or application. Examples include: MS Copilot, ChatGPT, and Grammarly. AI Tools include both non-enterprise AI Tools and Enterprise AI Tools.

Appointing Authorities are the Presiding Judge, Judicial Branch Administrator, Chief Adult Probation Officer, and Chief Juvenile Probation Officer.

Enterprise AI Tool is an AI Tool for which there is an agreement between the software vendor and Judicial Branch that requires protection of the information entered into the tool by Judicial Branch Users, along with protection of the information generated by the tool. This is to ensure information is secured and not shared. Additional terms used to describe an Enterprise AI Tool are Sequestered System and Sequestered Tool.

AI Restricted Information refers to Judicial Branch data, documents, AI-generated content, or records that may be in the form of text, images, video, sounds, or any other medium that must be protected in accordance with the Judicial Branch Information Security Policy. The Judicial Branch defines AI Restricted Information as follows:

Case Records refers to:

(1) any record that is collected, received, or maintained by a court or clerk of court in connection with a judicial proceeding;
(2) any order, judgment, or minute entry that is related to a judicial proceeding; and
(3) any index, calendar, docket, or register of actions associated with a case or in connection with a judicial proceeding.

Closed or Confidential Information refers to records in the custody of the Judicial Branch that the public may not inspect, obtain copies of, or otherwise have access to unless authorized by law or court order. Records are designated as "closed/confidential" by Arizona Rules of Court-including Supreme Court Rule 123-as well as by statute. Examples include Judicial Branch personnel records, judicial work product, adult and juvenile probation files, sealed records, and certain types of case records that are designated as "closed/confidential" by rules of procedure or statute.

Non-Public Judicial Branch Administrative Records refers to the following records pertaining to the administration of the courts or systems that are confidential pursuant to Supreme Court Rule 123:

(1) Employee/Human Resources records
(2) Employment applicant records
(3) Security records
(4) Procurement records as specified
(5) Preliminary and draft reports concerning court operations
(6) Law Library Resource Center patron records
(7) Attorney and judicial work product
(8) Juror records
(9) Proprietary and licensed materials
(10) Judicial Branch training records
(11) Records regarding remote electronic access to court records

(12) Records relating to the operation of the court computer network, automated data processing, or telecommunications systems
(13) Records concerning technical and physical infrastructure supporting courts or court systems.
(14) Juvenile Probation Department records concerning juvenile probationers
(15) Adult Probation Department records concerning adult probationers

Sensitive Information refers to full names, social security numbers, driver's license numbers, bank account numbers, credit card numbers, any other financial account or personally identifying information (PII) or protected health information (PHI), and any other content deemed sensitive by court rule or statute.

Information Security is the practice of protecting information, systems, and networks from unauthorized access, disclosure, alteration, or destruction to ensure the confidentiality, integrity, and availability of information.

Information Security Office (ISO) is a unit within the Judicial Branch's Court Technology Services Department responsible for the confidentiality, integrity, and security of Branch Technology Resources pursuant to the approval of the Presiding Judge.

Large Datasets refer to extensive collections of data that are too vast or complex to be effectively analyzed using traditional data processing methods. These datasets may include large volumes of information, often encompassing a variety of data types (e.g., structured, unstructured, numerical, textual) that require specialized tools, such as AI technologies, for analysis. The datasets can be large in terms of data size (terabytes, petabytes, etc.) or the complexity of patterns and relationships they contain, and their analysis may involve advanced techniques like data mining, machine learning, or natural language processing.

Personally Identifiable Information (PII) is any information that (a) can be used to establish a link between the information and the natural person to whom the information relates, or (b) is or can be directly or indirectly linked to a natural person.

Personnel or Employees are people paid a wage or salary from public monies in accordance with official entries on the payroll system for the Judicial Branch. This includes all classified, unclassified, temporary, exempt, non-exempt, and contract employees. This does not include contractors or third parties.

Sequestered System or Tool is an AI system in which the vendor protects the confidentiality of user input and prompt data, meaning it is not shared or made available to external parties.

User is a person with access to the Judicial Branch network or Information Processing Services. (This includes contractors and third parties.)

IV. POLICY

A. Use of Artificial Intelligence Tools

1. Unless otherwise restricted or prohibited, Judicial Branch Users may utilize non-enterprise AI Tools for Judicial Branch work-related activities.
2. Judicial Branch Users are prohibited from using AI Restricted Information in any AI Tool unless the tool is expressly authorized on the *Artificial Intelligence Tool List* or its use is permitted in an Enterprise AI Tool in accordance with Section C(1).

3. To minimize risk to the Branch, the following applies when using AI Tools:
    a) Prior to using AI Tools for Judicial Branch work-related activities, Users must complete, on an annual basis, "Judicial Branch Security Awareness and Guidelines" training via the Learning Management System ("the HUB") to understand the risks associated with the use of AI Tools, and Users must remain compliant with the Information Technology Acceptable Use Policy (Policy CS-143) and ensure they have signed the Acceptable Use Policy Agreement.
    b) If using AI Tools to perform Judicial Branch work-related activities, Users must register in the tool with their Judicial Branch email address.
    c) The Information Security Office may, upon determination of cause, block any AI Tool deemed an unacceptable risk to the Judicial Branch.
    d) Users must understand the limitations of AI and exercise caution when relying on its output. AI-generated content must be reviewed for accuracy, clarity, completeness, relevance, bias, ethical considerations, legal/regulatory compliance, and any other potential issues.
    e) Users are ultimately responsible for appropriate use of content generated by AI Tools.
    f) Users will not use AI Tools to misrepresent themselves, the Branch, or Judicial Branch Personnel.
    g) When using AI Tools, Users must comply with relevant laws, legal standards, court policies, and ethical and professional conduct rules, including, but not limited to, the Code of Ethics for Court Staff (Policy HR-312).
    h) Users must report data breaches or inadvertent disclosures of AI Restricted Information to their supervisor and to the Judicial Branch Information Security Office immediately.

B. Review of AI Tools Not Authorized on the Artificial Intelligence Tool List

1. Judicial Branch Users wishing to use any AI Tool for work-related activities not listed on the *Artificial Intelligence Tool List* attached to this policy as Addendum "A" must seek and receive approval before using the tool. Requests must be made through Court Technology Services to the Information Security Office.
2. The Information Security Office will review the request and assess the following factors:
    a) The security of the software and the third party, based on the established Security Standards for Third Party Risk Management and associated procedures;
    b) Where User input or uploaded information is processed and stored;
    c) Whether User input or uploaded information is made available to the public;
    d) How the third party is authorized to use the information; and
    e) The security of information transmission.
3. Upon completion of the review;
    a) The Information Security Office will notify the Chief Information Officer of their findings and recommendation.
    b) The Chief Information Officer will discuss the findings with the Presiding Judge and Judicial Branch Administrator.

c) The Presiding Judge will make the final decision to allow or disallow use of the requested AI Tool.

C. Request for Enterprise AI Tools

1. The following individuals are eligible to receive a Microsoft Copilot enterprise AI license upon submitting a request via ServiceNow: full-time judges and commissioners, staff attorneys, and other Judicial Branch Users identified by the Presiding Judge.
2. Users not categorically identified above in Section C(1) of this policy may request permission to obtain an enterprise AI license by submitting a software request via ServiceNow. When submitting the ServiceNow request, the user should include information regarding the intended use of the AI Restricted Information. Enterprise **AI** license requests must receive the following approvals: (1) the requesting User's Department Administrator/Division Director; (2) the Legal Department; and (3) the appropriate Appointing Authority.
3. The retention of an enterprise AI license is subject to review.
4. Before using an enterprise AI license, Users must complete mandatory training on the ethical considerations, data privacy laws, and the organizational practices governing data research and analysis. Authorization for use of Enterprise AI Tools will be provided upon certification of completed training.

D. Case-Use of Enterprise AI Tools

1. Users are prohibited from using Enterprise AI Tools or platforms to conduct any form of research, analysis, or data processing involving Large Datasets without prior approval from the Legal Department, the appropriate Appointing Authority, and the Presiding Judge. This includes, but is not limited to, performing AI-based predictive modeling, trend analysis, or creating AI-generated reports that involve large-scale or sensitive organizational data.
2. Any employee intending to use Enterprise AI Tools for large data analysis must submit a formal request to the Legal Department detailing the purpose, scope, and expected outcomes of the research. The Legal Department will review the request with the appropriate Appointing Authority and the Presiding Judge. The approval process will involve an evaluation of the potential risks, ethical considerations, and data privacy concerns, and will assess whether the use of Enterprise AI Tools aligns with organizational objectives and policies.
3. Users found using Enterprise AI Tools for unauthorized research or data analysis may be restricted from further use of Enterprise AI Tools and/or subject to disciplinary action.

E. Development of AI Tools

1. The in-house development of AI Tools requires the approval of the Presiding Judge.
2. Requests for in-house development of AI Tools must follow existing Judicial Branch procedures for requesting new Court Technology Services projects and include a project plan that identifies goals, benefits, estimated cost and a timeline of the project. Additionally, and as defined in Section B(2) of this policy, the Information Security Office shall conduct a review to be addended to the project plan. AI Tools must be developed in accordance with the Secure Coding and Testing Standards.
3. The Chief Information Officer shall adopt procedures for regularly reviewing all models for accuracy and completeness.

V. COMPLIANCE

Any person subject to these standards who fails to comply with the provisions as set out above, or any amendment thereto, may be subject to appropriate disciplinary or legal action as follows, if applicable:

1. Financially responsible for any loss or damage caused by non-compliance with Judicial Branch Information Security policies, standards, protocols, and requirements;
2. Disciplinary action, up to and including termination of employment;
3. Loss of access to/use of AI Tools.

VI. ARTIFICIAL INTELLIGENCE GOVERNANCE

The Judicial Branch, via Administrative Order, created the Artificial Intelligence Committee to act as the central clearinghouse for all artificial intelligence matters for the Judicial Branch in Maricopa County.

At minimum, the Committee shall be responsible for the annual review of this Policy and, as necessary, recommend to the Presiding Judge updates and modifications to ensure the safe and continued use of **AI** Tools. The review and recommendations should include, but not limited to, updating the Artificial Intelligence Governance Policy to account for emerging threats, new technologies and opportunities, and changing regulatory requirements.

Addendum "A" to CS-144, AI Governance Policy
Artificial Intelligence Tools List

This list has three sections: 1. Approved Tools for Use with Limitations, 2. Approved Tools for Use with No Limitations, and 3. Prohibited Tools. Each section includes applicable procedures.

This list is reviewed and updated regularly by the JBAZMC Information Security Office (ISO) and maintained on the Information Security Office's page on SharePoint.

1. APPROVED Tools for Use - AI Restricted Information Prohibited

These tools may be used with information NOT defined as AI Restricted Information as defined in the Artificial Intelligence Security Standards. A list of these records is in CS-144 Artificial Intelligence Governance Policy. If using these tools for JBAZMC work-related activities, Users must use their JBAZMC email address if registration is required to use the tool.

AI TOOL	AI FUNCTION
Adobe Express	• Assist in design creation and image editing • Automated layout and content suggestions
Adobe Firefly	• Generative creative content (images, text effects) • Text-to-image generation and image editing
Adobe Sensei	• Machine learning across Adobe apps • Automated tagging, image recognition, content insights
Anyword	• Copywriting and text optimization • Performance prediction for marketing messages
Beyond Words	• Voice generation and text-to-speech • Voice cloning and synthesis for multimedia applications
Builder.io	• Assisted website and UI design • Drag-and-drop page building with smart design recommendations
ChatGPT	• Conversational assistant with natural language understanding • Text generation, question answering, creative content support
Coveo	• Search and recommendation engine • Personalized content delivery and data insights
Freepik	• Enhanced search and curation of graphics • Intelligent categorization of design resources
Grammarly	• Writing assistant for grammar and style checking • Tone detection and plagiarism prevention
IVY	• Conversational support for customer engagement • Automated interactions and personalized responses
LanguageTool	• Grammar and style checking • Error detection and writing improvement suggestions
Microsoft Designer	• Graphic design with text-to-image generation • Automated layout and creative template suggestions
Microsoft Copilot Chat	• Conversational assistant integrated into Microsoft products • Natural language support for tasks, document summarization, and coding
Perplexity AI	• Question answering and search • Concise responses with citation-based references

Quig	• Content and copywriting support • Generation and summarization of ideas and text
Quizlet	• Adaptive learning tools • Personalized flashcards and content recommendations
ReadSpeaker	• Text-to-speech conversion • Voice synthesis for accessibility and multimedia applications
Wordtune	• Writing assistant for rephrasing and rewriting • Suggestions for tone, style, and clarity improvements
Yellow AI	• Conversational automation through chatbots and virtual assistants • Multi-channel customer support and engagement solutions

Section 1 Procedures:

- If User already has access, no action is needed. User must use JBAZMC email address if performing JBAZMC work-related activities.
- If User needs an AI Tool that requires a license, submit a "Software Request" ticket in ServiceNow with supervisor's approval. The granting of a license for an AI Tool listed in Section 1 does not give the User permission to use AI Restricted Information with the AI Tool.

2. APPROVED Tools for Use with AI Restricted Information

These tools, if used with an Enterprise license, are sequestered, meaning the information entered into the tool will not be shared outside of JBAZMC. There is no limitation on the use of AI Restricted Information with these tools; however, the use of these tools must comply with the Case-Use restrictions in the Artificial Intelligence Governance Policy, CS-144.

AI TOOL	**AI** FUNCTION
ChatGPT Enterprise Version	• Enterprise-grade conversational assistant • Enhanced data privacy and business tool integration
Adobe Firefly Enterprise Version	• Generative creative content tailored for commercial workflows • Streamlined integration into enterprise design processes
Microsoft 365 Copilot	• Conversational assistant integrated into Microsoft 365 • Enhanced productivity and task automation
Westlaw Precision	• Legal research and document analysis • Intelligent search and insights for legal professionals

Section 2 Procedures:

- If User already has access, no action is needed. User must use JBAZMC email address if performing JBAZMC work-related activities.
- If User has business need for an AI function and the AI Tools above do not satisfy the business need, submit a "Software Request" ticket in ServiceNow with supervisor's approval.

3. PROHIBITED for Use at JBAZMC

These tools pose an unacceptable level of risk to JBAZMC and are therefore prohibited from use and/or for performing JBAZMC Work.

AI TOOL
Deepseek
MidJourney
Section 3 Procedures. • If User is of the opinion a tool should not be used by JBAZMC Personnel because it presents an unacceptable level of risk, send an email to ITGovernance@jbazmc.maricopa.gov for review. • If User is of the opinion a listed in this section should not be on the prohibited list, send an email to ITGovernance@jbazmc.maricopa.gov for review.