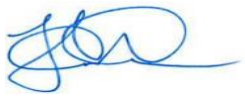
DESCHUTES COUNTY SHERIFF'S OFFICE

Policy Title: **USE OF ARTIFICIAL INTELLIGENCE (AI)**	Effective Date: September 12, 2024		Policy Number: **4.35**
Accreditation Reference:	Review Date: September 12, 2027	Supersedes: New	Pages 4
Attachments:	 L. Shane Nelson, Sheriff		

I. STATEMENT OF POLICY

Generative Artificial Intelligence (AI) refers to technology that can generate human-like text, images, or other media content using AI algorithms. These tools are sophisticated models that predict the language, text, audio, or video that satisfies input.

The Deschutes County Sheriff's Office recognizes the transformative potential of generative AI technologies in shaping the future of our business landscape. The Sheriff's Office will regularly review and update this policy to keep it aligned with ethical and legal standards and technological advancements in AI as frequently as needed.

The purpose of this policy is to provide a set of guidelines and best practices for the responsible, ethical, legal, and secure use of AI within the business operations of the Sheriff's Office. This policy details the requirements that members, volunteers and others acting on behalf of the Sheriff's Office must follow when using generative AI tools, including the security risks and the protection of confidential data.

This policy designates two approved real time request/response generative AI systems for the Sheriff's Office. All other generative AI systems must receive approval from the Sheriff's Office IT before use.

II. DEFINITIONS

1. GENERATIVE AI:

   (a) Real time request/response (Online-based) - generative AI that users can interact with in real-time through the internet, providing immediate responses to their queries,

requests or prompts using generative AI techniques. This type of AI could be used in various applications such as chatbots (ChatGPT, Microsoft Copilot, Claude, etc.), content generation platforms, customer support systems, image creation, and more.

(b) Software embedded generative AI[1] - Integration of generative AI algorithms directly into software or hardware systems, allowing them to autonomously create content, make decisions, or generate outputs based on certain inputs or parameters (virtual meeting notetakers, Slack AI, etc.). This type of AI is designed to operate within constrained environments, such as Internet of Things "IoT" devices, mobile apps, or embedded systems in various machines.

III. APPLICABILITY

This policy applies to all officials, members, volunteers, and others acting on behalf of the Deschutes County Sheriff's Office who use generative AI tools or platforms. This policy includes both online-based generative AI, which functions in a real time request/response format, as well as embedded generative AI which comes built into many software platforms.

Unless specifically directed by their supervisor, members are not required to use AI systems and tools. Members of the public should be informed when they are interacting with an AI tool and have an alternative to using AI tools made available to them.

IV. POLICY AND PROCEDURE

1. Use of AI Systems and Training

When creating accounts with approved AI providers for generative AI tools, Deschutes County Sheriff's Office staff have the option to use either their official DCSO email address or their personal email address.

All members are required to complete the AI training in the Sheriff's Office eLearning portal before using AI for work-related purposes on Sheriff's Office computing resources.

2. Approved AI Systems

There are two approved AI real-time request/response systems for use at the Deschutes County Sheriff's Office:

1. ChatGPT (OpenAI)
2. Co-pilot (Microsoft)

Any use of non-approved AI systems on Sheriff's Office computing resources is strictly prohibited. Contact Sheriff's Office Information Technology to have their staff review and approve the use of additional AI systems.

[1]Embedded AI may be more difficult to recognize. If there are questions about AI types, please reach out to Deschutes County Sheriff's Office IT staff for assistance.

Members are responsible for staying updated on any changes to the platform's policies or terms of use regarding generative AI. They should also keep informed about developments in AI technology and how they may impact their usage.

3. Software-Embedded Generative AI

(a) Prior to utilizing or enabling generative AI embedded in any software platform on Sheriff's Office computing resources, IT shall be consulted to assist with security recommendations, configurations, and best practices.
(b) Members must not give access to Sheriff's Office AI tools outside the organization or allow external AI tools to have access to DCSO resources (E.g., AI Notetaker Bot) without prior approval from Deschutes County Sheriff's Office IT.
(c) Members must not share their access credentials or allow unauthorized individuals to use the generative AI tools on their behalf.
(d) Generative AI tools and platforms must be configured securely, following industry best practices and vendor recommendations. This includes ensuring the latest updates, patches, and security fixes are applied in a timely manner.
(e) Any software containing embedded AI must follow Deschutes County Sheriff's Office password policy. The recommended authentication is through Single Sign On which can be set up by Sheriff's Office IT.

4. Data Privacy and Security

Currently, the Sheriff's Office does not have access to any generative AI tools or platforms in which the data input/output is governed by the Sheriff's Office. Therefore, care must be taken when utilizing generative AI tools or platforms, especially when that use involves Sheriff's Office data.

(a) Efforts should be made to anonymize data, eliminating any elements that could be traced back to the Sheriff's Office.
(b) Members must adhere to Deschutes County Sheriff's Office data, privacy, and security standards, State and Federal laws, Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information System (CJIS), Personally Identifiable Information (PII), and Protected Health Information (PHI) when using AI systems.
(c) Using restricted or confidential organizational data with AI is prohibited. Members must not upload or share any data that is confidential, proprietary, or protected by compliance / regulation. This includes data related to customers, members, or partners.

All members of generative AI must comply with Sheriff's Office acceptable use ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas.

Members must respect and protect intellectual property rights, both internally and externally. Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.

All members must familiarize themselves and comply with all terms of use (e.g. licensing agreements, privacy policies, codes of conduct, etc.) of the generative AI tool that they utilize.

Members must notify IT if/when they are in violation of terms and condition of use of the AI tool that they utilize or if they are notified of a violation of terms of use from an AI tool.

It is the sole responsibility of members who use AI generated output in their work product to ensure its accuracy and compliance with Sheriff's Office policies and all applicable laws. Members will be held solely responsible for any AI generated output that results in such violations.

5. Responsible Use

Members are responsible for ensuring that the generated content produced using generative AI is accurate and aligns with the organization's values, ethics, and quality standards. Generated content must not be used if it is inaccurate, misleading, harmful, or offensive. Any AI generated product utilized by a member will be deemed adopted by the member and treated as the member's individual work product.

Members must actively work to identify and mitigate biases produced by AI systems. They should ensure that the output utilized from the AI systems is fair, inclusive, and does not discriminate against any individuals or groups. Members will be held solely responsible for any AI output that is utilized in their work product that is biased or discriminatory.

AI tools can generate inaccurate and false information. Members should fact check, and review content generated by AI. Members are responsible for the outcomes generated by AI systems and should be prepared to explain and justify those outcomes. Members shall not retain any records of queries and are required to delete all chat history in the AI tool they utilize immediately.

6. Cybersecurity

Any suspected or confirmed cybersecurity incidents related to generative AI usage should be reported promptly to the Sheriff's Office IT Unit. Examples could include unsolicited links with responses, unknown or unverifiable scripts or code, suggested downloads from chat bots, and requests for restricted data.

7. Unlawful Activities

Members must report any suspected violations of this policy or any potential ethical, legal, or regulatory concerns related to AI use to their supervisor.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and legal consequences, if laws are violated.