OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Artificial Intelligence (AI)	ISD_650_01
Supersedes: None		
Applicability: All state employees (their agents), volunteers, vendors, and contractors, including those affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives.		
Reference: None		
Effective Date: February 26, 2024		Approved: 

I. PURPOSE

The purpose of this policy is to establish the acceptable use and expectations of generative and embedded Artificial Intelligence (AI) within Oregon Department of Fish and Wildlife (ODFW).

II. DEFINITIONS

A. **Copyright:** Laws to control all use of an original work, such as a photograph, picture, book, movie, music, or software for a particular use or time.

B. **Embedded AI:** The ability of a product, process, or service to act on its own based on operational or environmental information collected via embedded sensors.

C. **Generative AI:** Generative artificial intelligence (AI) uses advanced technologies such as predictive algorithms, machine learning, and large language models to process natural language and produce content in the form of text, images, or other types of media. Generated content is typically remarkably similar to what a human creator might produce, such as text consisting of entire narratives of naturally reading sentences. May include systems such as chatbots (ChatGPT, Google's Gemini, Microsoft Bing) or image generators (DALL-E 2, Midjourney)

D. **Information Technology (IT) Assets:** Any data, application, computer, peripheral, portable computing device, or other technology used to store, transport, modify, display, or

report information that has value to the organization regardless of its physical form or characteristics.

E. **Intellectual Property:** a work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights, patent, copyright, or trademark.

F. **Machine Learning:** The ability of a computer or system to learn and adapt without following explicit instructions by using algorithms and statistical models to analyze patterns in data.

G. **Security:** The practice of preserving integrity availability and confidentiality of information through the use of access controls, encryption, and other forms of technologies along with training, audits, and policy.

H. **User:** All state employees (and their agents), volunteers, vendors, and contractors, including those users affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives.

I. **User ID:** The user identification used to authenticate to a computing device or network.

III. Background

Generative AI tools have the potential to enhance productivity by assisting with tasks such as drafting documents, creating content, generating ideas, solving problems, and coding software. However, AI technologies also come with potential risks that include inaccuracies, bias, and unauthorized use of intellectual property within the content generated. In addition, the public availability of information submitted as input to AI could pose security or privacy concerns for the agency.

The ongoing adoption and acceptance of AI within ODFW will depend significantly on employees' ability to demonstrate the use of AI is valid, reliable, safe, secure, resilient, accountable, transparent, explainable, fair, and without harmful bias.

IV. POLICY

The use of Artificial Intelligence (AI) is for business productivity and research that aligns with the agency's mission, principles, goals, and values in a manner that fosters public trust, promotes good science, and instills confidence in the use of AI with coworkers, constituents, partners, and the public. The use of any AI content or systems must be consistent with all applicable laws and state policies.

A. Applicability

This policy applies to existing and new uses of AI within the agency, stand-alone AI and AI embedded within systems or applications, AI developed both by the agency or by third parties on behalf of agency, all relevant data inputs used to train AI, and AI information outputs used in support of agency work.

B. Authorized Use

The use of generative and embedded AI tools and systems are for business purposes only and within the scope of the employee's duties. Additional authorization or security configurations may be required by the Department of Administrative Services (DAS) or Information Services Division (ISD) according to the typical thresholds for all other IT services and procurements.

C. Personal Use

The personal use of AI tools or systems on state information assets is prohibited including the time before or after work, during breaks, or lunch. The use of AI tools and systems are exempt from the limited and incidental personal allowances as described in ISD_601_01 'Acceptable Use of Information Systems'.

D. Ethical Use

Employees must use generative AI in accordance with the agency's code of conduct and acceptable use policies. AI must not be used to create content that is inappropriate, hateful, discriminatory, or otherwise harmful to others or the agency.

E. Confidential Information

Employees must not input or share data that is confidential, proprietary, sensitive, or protected by policy or regulation with any external AI system. This includes information or data that contains information with asset classification L3 'restricted' or L4 'critical' or any other nonpublic agency information that might be harmful to the agency if disclosed. Prior to use of information with an asset classification of L2 'limited', verify with the data owner for any limitations.

F. Validate Information

Responses from generative AI outputs must be reviewed by knowledgeable subject matter employee(s) for accuracy, appropriateness, privacy, and security before publishing or utilization for any purposes. A user who utilizes generative AI to draft content is ultimately accountable for the quality and suitability of the content for business use.

Responses generated from generative AI must <u>not</u> be:

a. assumed to be accurate, credible, or truthful until verified or authenticated.
b. used verbatim where such use would violate copywrite or intellectual property rights.
c. used as a single authoritative source for decisions or actions.
d. used to issue official statements (i.e., policy, legislation, or regulations) without extensive review and approval by management.
e. used to impersonate individuals or organizations.
f. used for any activities that are harmful, illegal, or in violation of code of conduct or agency acceptable use policies.

G. Harmful Bias

Responses provided by generative AI are based on patterns and examples from the data it has been trained on rather than representing the opinions or official stance of the agency. Employees are expected to review and edit all generative AI responses to address any biases that may emerge during

use. Bias may be expressed in opinion but also in data. It is the responsibility of the employee to ensure accuracy, fairness, and equity.

H. Application Development / Software Code

Software code developed by generative AI shall only be implemented after identifying and mitigating all business and security risks related to its use, including electronic scanning of derived code for vulnerabilities. All use of AI generated software code must be annotated with source and intended function.

I. Data Privacy and Security

Embedded AI systems must be implemented with strong data privacy and security measures in place. This includes implementing encryption protocols and complying with relevant state and agency policies including data protection laws. Any AI with embedded facial, voice, fingerprint, or other biometrics must align with established policy and practices of the state for security and privacy.

The use of generative AI systems must comply with state security standards and protocols with established reputations and recognized as industry technology leaders in AI development.

J. User Access and Control

Employees must apply the same security best practices with AI as for all other agency systems. If login credentials are required, account names and passcodes must align with established security policy and practices of the agency. As applicable, least rights privileges must also be applied.

K. Legal Compliance

The use of generative AI must comply with all applicable laws and regulations, including data protection, privacy, and intellectual property laws. Unauthorized use of copyrighted material or the creation of content that infringes on the intellectual property rights of others is strictly prohibited. Users shall read and comply with the Terms of Service (TOS) and associated linked documents prior to using any AI tool or service.

L. Audit

The agency may monitor and audit the use of generative AI to assure proper use and appropriate safeguards are applied.

V. POLICY GROUP

This policy is part of a suite of ODFW Information Technology policies that collectively sets the expectations and use of computing devices and related technology under the main policy ISD_610_01 'Acceptable Use of Information Systems'.