FEEDBACK

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Responsible Use of Artificial Intelligence (AI)

APS Number: 6012 **APS Functional Area:** INFORMATION TECHNOLOGIES

Brief Description:	CU is committed to leveraging AI innovations while protecting privacy, ensuring security, and upholding transparency, fairness, and human oversight in alignment with its mission and values.
Effective:	TBD
Approved by:	President Todd Saliman
Responsible University Officer:	Associate Vice President and Chief Information Officer
Responsible Office:	University Information Services
Policy Contact:	University Information Services
Supersedes:	N/A
Last Reviewed/Updated:	N/A
Applies to:	Universitywide

Reason for Policy: To promote responsible and secure use of AI across the University of Colorado ("University" or "CU"), ensuring that AI technologies are used in ways that protect individual rights, data, and security and advance the University's mission. Governance authority rests ultimately with the President and Chancellors; this Policy ("Policy") provides necessary governance structures and outlines campus requirements for digital accessibility.

I. INTRODUCTION

Advances in Artificial Intelligence ("AI") offer significant opportunities to enhance teaching, learning, research, and administration at CU. At the same time, the use of AI presents new and evolving ethical, legal, and operational challenges. The university recognizes both the promise and the risks of AI and is committed to maximizing the benefits of AI in support of its mission, while mitigating potential harm.

Multiple federal and state laws and regulations apply to the use of AI systems, particularly regarding data protection, privacy, and non-discrimination. For example, the use of AI systems must comply with student privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and state privacy laws.

The use of AI systems for University academic, research or administrative activities ("University Activities") must comply with CU's data security, privacy, and intellectual property policies, even when such use occurs outside CU's direct visibility or control; in research or specialized contexts, separate agreements may govern AI systems use and should be harmonized with this Policy.

II. POLICY STATEMENT

A. <u>Scope and General Requirements:</u> This Policy governs the use of AI systems for University Activities by all CU students, faculty, staff, and other affiliates ("Users"). All use of AI systems at CU must comply with applicable laws, regulations, and University policies. This includes, but is not limited to, laws and policies on data privacy, data governance, information technology ("IT") security, accessibility, intellectual property, and academic integrity. Key applicable CU policies and practices include:

1. Acceptable Use Policies: Users of AI systems must adhere to campus IT acceptable use policies which require ethical and legal use of IT resources.

2. APS 6005 – IT Security Program: CU's baseline security standards (APS 6005) apply to AI systems and data. Users must protect University data when using AI systems. No confidential, highly confidential, highly sensitive, or regulated data (including but not limited to Social Security numbers, financial account numbers, driver's license/state IDs, health/medical records, FERPA-protected student information, legally protected research data, or other data classified as "Restricted" under APS 6010) shall be entered into any AI system that is not University-approved for such data. Users and departments deploying AI systems must ensure security controls are in place consistent with APS 6005 and do not circumvent any security requirements. Using an AI system does not exempt one from requirements to protect restricted data.

3. APS 6010 – Data Governance: AI systems that handle University data must comply with CU's data governance and data classification requirements (APS 6010). Institutional data input to or output from AI systems should be managed as "data assets" per APS 6010. In practice, this means data used by AI systems must be classified (e.g., public, confidential, or highly confidential) and protected accordingly. Data outputs from AI systems that are retained (such as an analysis or a decision record) become University records and should be managed per relevant records retention policies and data governance rules. The input of confidential and/or highly confidential data into AI systems not approved for use by campus IT is strictly prohibited.

4. APS 2027 Code of Conduct: AI system use at CU should reflect the University's commitment upholding the highest ethical, professional, and legal standards. AI systems should not be used in ways that violate anti-discrimination laws or CU's policies on discrimination and harassment.

5. Academic Integrity: Unauthorized use of AI systems to produce academic submissions is considered Academic Misconduct unless expressly permitted by the instructor or the University. Decisions about the use of AI systems in coursework and classroom activities are made at the discretion of individual faculty members. Instructors may establish their own expectations and guidelines for AI use in each course, and students are responsible for adhering to those rules. Each campus may provide additional guidance on acceptable versus unacceptable academic uses of AI, consistent with this APS.

6. Synthetic Media and Deepfakes: Any use of Synthetic Media (including Deepfakes) in official University content must be clearly disclosed. Deepfake representations of individuals must not be created or distributed without their explicit, informed consent, unless the use is part of:

   - Structured academic work under faculty supervision, such as coursework, research, or creative projects in disciplines like art, media studies, history, or digital design.
   - Educational content that depicts public or historical figures for instructional clarity, satire, or social commentary, provided the context is clearly communicated and the intent is not misleading.

   In all cases, Synthetic Media must be used responsibly, with appropriate context and transparency to avoid confusion, misrepresentation, or harm.

7. Other Applicable Policies and Practices:

   a. Protected Health Information (PHI) and other regulated data (like Health Insurance Portability and Accountability Act ("HIPAA")-governed data) can only be processed by AI systems consistent with specific regulations.

   b. AI-derived content used for official communications must also comply with branding, communication, and web policies as relevant.

   c. University data, including information related to students, faculty, and staff, must not be used to train commercial artificial intelligence models, except in cases where such use is approved by the University in accordance with AI campus governance and in compliance with applicable privacy regulations and data governance policies.

B. AI Governance Structure: Each campus[1] Chancellor (or designee) shall establish and maintain an AI governance structure to oversee implementation of this Policy on their campus. At minimum, each campus will: (1) designate a responsible office or officer (e.g., the Chief Information Officer or a committee chair) to coordinate AI systems policy compliance and education; (2) develop campus-specific AI policies or procedures that align with this APS and address local needs and (3) ensure that processes exist for reviewing and approving high-risk AI system use cases (such as enterprise-level AI systems or any AI systems that will handle highly sensitive data or make autonomous decisions affecting individuals).

1. Campus Committees**:** Campuses will be responsible for developing campus AI guidelines, reviewing proposals for new AI systems, and monitoring AI systems use on campus. This committee will review and approve high-risk AI systems intended for use exclusively on a single campus. The committee will meet regularly to evaluate AI-related opportunities and risks, and to share best practices.

2. Systemwide AI Committee: The systemwide Responsible Officer (AVP & CIO) or designee will convene a System AI Committee ("Committee") with at least one representative from each campus's AI committee structure. The purpose of this Committee is to serve as a centralized support and coordination body. It will facilitate sharing of information and resources across campuses, develop or disseminate common guidance (e.g., templates for AI risk assessment, lists of approved AI tools), and help ensure consistent AI policy enforcement. In collaboration with the University's shared governance, this Committee will review high-risk AI systems proposed for systemwide use and follow CU's IT Governance approval process. The system committee should meet at least annually, and additionally as needed, to review the overall state of AI use at CU and recommend any updates to this Policy.

C. Transparency, Accountability, and Explainability: The University of Colorado commits to a transparent and human-centered approach to AI - defined as AI systems designed to support human judgment, uphold academic values, and foster inclusive, transparent innovation. To that end:

1. Disclosure of AI Involvement: The use of AI in producing any official University content or communication should be disclosed, where appropriate.

2. Human Oversight and Decision Authority: AI systems do not supersede human responsibility. Any AI recommendation or decision that has significant effects on individuals or major institutional outcomes (for example, an AI system flagging research misconduct, or an AI system shortlisting job applicants) must be subject to human review and judgment before final action. The University emphasizes "staying human-first," meaning AI systems should augment human decision-makers.

3. Accountability and Incident Response: If an AI system produces an incorrect, harmful, or inappropriate outcome (e.g., breaches data privacy, yields a biased decision, or malfunctions in a critical process), the incident must be promptly reported to the appropriate authority (such as the campus IT Security Office, Compliance Office, or AI committee). The University will address such incidents like other Policy violations or IT incidents: investigating the cause, mitigating any harm, and adjusting practices or systems to prevent recurrence.

III. DEFINITIONS

A. Artificial Intelligence (AI) System: Any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

B. Synthetic Media: Refers to content—such as images, video, audio, or text—that is generated or manipulated using artificial intelligence rather than captured or produced by traditional human methods.

C. Deepfake: AI-generated synthetic media (e.g., video, audio, or images) that convincingly mimics real individuals or events, often with the intent to deceive or mislead.

D. High-Risk AI System (as defined by SB24-205): Any AI System that, when deployed, makes, or is a substantial factor in making, a consequential decision.

Note: Other technical terms (data classifications, etc.) are as defined in APS 6005 and APS 6010 if not re-defined here.

IV. RELATED POLICIES

A. APS 5065 - Protected Class Non-Discrimination
B. APS 6005 - IT Security Program
C. APS 6010 – Data Governance
D. APS 2027 – Code of Conduct
E. Campus IT Acceptable Use Policies
F. Colorado SB24-205

V. HISTORY

- Adopted: TBD.
- Revised: N/A.
- Last Reviewed: N/A.