NUMBER: 1220

TITLE: Standards for the Safe Use of Artificial Intelligence

APPROVED: April 19, 2024

SCHEDULED REVIEW DATE: April 2029

A. PURPOSE

The purpose of this policy is to establish a culture of integrity that ensures the responsible, ethical, transparent use of artificial intelligence (AI) technology in public higher education by implementing comprehensive AI standards across the University ecosystem.

B. AUTHORITY

Virginia Code Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 7.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to university operations.

Executive Order Number Thirty (2024), Commonwealth of Virginia, Office of the Governor, Implementation of Standards for the Safe Use of Artificial Intelligence Across the Commonwealth

C. DEFINITIONS

Artificial Intelligence (AI): Refers to the simulation of human intelligence processes by machines, particularly computer systems. This encompasses various techniques such as machine learning, natural language processing, and computer vision, enabling systems to perform tasks that typically require human intelligence.

Ethical Use: Prioritizing moral considerations and principles in the deployment of AI, emphasizing fairness, accountability, and transparency in all AI applications.

Equity: Ensuring fairness and equal access to AI resources and opportunities for all individuals, regardless of background or demographics.

Learning Experience Enhancement: Leveraging AI technologies to personalize learning experiences, cater to diverse learner needs, and improve student outcomes.

Privacy Protection: Measures aimed at safeguarding the confidentiality and security of individuals' data, ensuring compliance with relevant state and federal regulations.

Risk Mitigation: Strategies to identify, assess, and manage potential risks associated with AI technologies, including biases, discrimination, and data breaches.

D. SCOPE

This policy applies to all Old Dominion University employees, including staff, administrators, faculty, full- or part-time, and classified or non-classified persons paid by the University. It encompasses the use of artificial intelligence (AI) technologies across various University activities, emphasizing responsible and ethical practices. This scope extends to AI applications in research endeavors, educational initiatives, administrative functions, and all other areas where AI technologies may be employed within the University ecosystem.

E. POLICY STATEMENT

Old Dominion University is committed to the effective implementation of comprehensive artificial intelligence policy standards that support research, teaching, and administration while safeguarding state business applications, protecting individual data, and mitigating risk. These standards will:

1. Ensure Ethical Use: Prioritize ethical considerations and ethical use in AI deployment, in teaching, learning, research, and administration, promoting fairness, accountability, transparency and respect for human rights in all AI applications and AI related activities conducted within the University.

2. Foster Innovation: Encourage innovation and experimentation in AI integration to enhance teaching, learning, and research outcomes.

3. Protect Privacy: Safeguard the privacy and security of individuals' data by implementing robust data protection measures in compliance with state and federal regulations.

4. Mitigate Risks: Implement strategies to mitigate risks associated with AI technologies, including biases, discrimination, and data breaches.

5. Promote Equity: Ensure equitable access to AI resources and opportunities for all students, faculty, and staff, irrespective of background or demographics.

6. Enhance Learning Experiences: Leverage AI technologies to personalize learning experiences, cater to diverse learner needs, and improve student outcomes.

F. PROCEDURES

1. The responsible office, the Division of Digital Learning, shall establish a standardized and transparent approval process for the acquisition, development, and/or deployment of AI technologies. The approval process requires the thorough review and ratification of AI technology by designated authorities in consultation with Procurement Services,

Information Technology Services, and other relevant University departments to ensure compliance with University AI policy.

2. Disclaimers and Transparency:

    a. All AI products or outcomes generated in educational settings must be accompanied by clear and comprehensive disclaimers that inform users about the limitations, assumptions, and potential biases of the AI system and clarify the roles and responsibilities of human users in interpreting and acting upon AI-generated information.

    b. Promote transparency in AI usage by providing stakeholders with access to information about AI applications and decision-making processes.

3. Mitigation of Third-Party Risks:

    a. Implement measures to assess and mitigate risks associated with third-party AI vendors, including vendor selection, data sharing agreements, contractual obligations, assessing vendor reliability, data security practices, adhering to ethical standards, by consulting with Procurement Services, and undergoing the University's software decision analysis process.

    b. Contracts with AI vendors should include provisions for data protection, privacy safeguards, in addition to clauses for non-compliance and dispute resolution by consulting with Procurement Services and following the software decision analysis process to ensure compliance.

    c. Conduct regular audits and assessments in collaboration with ITS to monitor the performance and security of third-party AI solutions.

4. Protection of Student and Employee Data:

    a. Implement robust data privacy and security measures to safeguard sensitive information collected or processed by AI systems.

    b. Ensure that AI systems comply with applicable laws and regulations governing the collection, storage, and use of student data, including the Family Educational Rights and Privacy Act (FERPA), the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other relevant state and federal privacy laws.

5. Protection of Research Data:

    a. Strengthen provisions related to data privacy and security when using AI technologies, adhering to best practices for protecting sensitive information and obtaining informed consent for data collection and analysis.

b. Implement measures to ensure that confidential, sensitive, and other protected data are not entered into any AI research tool without proper risk analysis. Protected data may include information protected by FERPA, HIPAA, confidential personnel records, intellectual property, Human and Animal Subject data, and other sensitive or confidential institutional research data.

c. Any use of AI tools in the research process using humans or animals should be disclosed in the Institutional Review Board (IRB) application and address potential ethical considerations.

6. Implementation: The implementation of AI Policy Standards within Old Dominion University will be supported by the following strategies:

   a. Training and Capacity Building**:** Provide training and professional development opportunities for faculty, staff, and administrators on AI ethics, best practices, and compliance requirements. Foster a culture of responsible AI usage through awareness campaigns, workshops, and educational resources.

   b. Collaboration and Partnerships**:** Forge partnerships with industry stakeholders, government agencies, and academic institutions to exchange knowledge, share best practices, and stay abreast of emerging trends in AI technology and policy. Establish interdisciplinary AI research projects to facilitate collaboration among researchers from diverse fields.

   c. Monitoring and Evaluation: Establish mechanisms for ongoing monitoring, evaluation, and review of AI initiatives to ensure alignment with AI Policy Standards and educational objectives. Solicit feedback from stakeholders and incorporate lessons learned into future AI projects and policies.

7. Community Engagement**:** Engage students, faculty, staff, and the broader community in discussions and forums on AI ethics, privacy, and societal implications. Foster dialogue and collaboration with local stakeholders to address community concerns and priorities related to AI integration.

8. The specific standards to be utilized for compliance with this policy are published on the Information Technology Services Computing Policies and Standards website. Additional guidelines are available on the University Web and Digital Communication website.

G. REGULAR POLICY REVIEWS

The Division shall conduct annual reviews of this policy to ensure its alignment with evolving regulations and best practices. These reviews shall involve consultation with experts, and other relevant stakeholders.

H. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the Commonwealth's Records Retention Schedules.

I. RESPONSIBLE OFFICER

Vice President for Digital Learning

J. RELATED INFORMATION

University Policy 3505 - Information Technology Security Policy
University Policy 3506 - Electronic Communication Policy for Official University Business
University Policy 3507 - Information Technology Accessibility Policy
University Policy 3508 - Information Technology Project Management
University Policy 3509 - Software Decision Analysis Policy
University Policy 4100 - Student Record Policy
University Policy 5350 - Research and Scholarly Digital Data Management Policy