University System of New Hampshire

ARTIFICIAL INTELLIGENCE (AI) STANDARD FOR THE UNIVERSITY SYSTEM OF NEW HAMPSHIRE

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity Governance Risk and Compliance (GRC)
Approved Distribution: PUBLIC
Status: IN FORCE

1 PURPOSE

This Standard outlines the principles and guidelines for the responsible use of Artificial Intelligence (AI) within the University environment. The purpose is to ensure that AI technologies are employed ethically, transparently, and in a manner that aligns with the University System's mission, values, and legal requirements.

2 SCOPE

This Standard applies to all administrative, academic, and business units at USNH and its component institutions.

3. AUDIENCE

All USNH community members with active relationships with USNH and its component institutions, including students, faculty, and staff, should understand the requirements outlined in this Standard.

4. STANDARD

4.1 ETHICAL CONSIDERATIONS

4.1.1 Human-Centric Approach: USNH, including all students, staff, faculty, and affiliates, will prioritize the well-being, safety, and dignity of individuals affected by AI systems. AI systems, and applications of them, must be designed and used in a way that respects human rights, privacy, diversity, and promotes inclusivity.

4.1.2 Privacy and Data Protection: USNH will comply with applicable data protection laws and safeguard personal information collected and processed through AI systems. Adequate measures must be implemented to protect data integrity, confidentiality, and user privacy.

Users of AI tools or programs must not share or enter any data classified as non-public (Tier 2 data and above), including but not limited to Personally Identifiable information (PII) or non-public research data. Sharing non-public institutional data with AI tools may result in unauthorized disclosure and result in data being potentially accessible by others. Please refer to the *USNH Information Classification Policy* for definitions of data tiers.

Individuals with questions about non-public data and the use of generative AI should consult University policies or contact the appropriate University data stewards for additional guidance.

4.1.3 Transparency and Understanding: AI systems developed or utilized by the University must be transparent, providing clear explanations and understanding of their capabilities, limitations, and decision-making processes. Users must have access to information regarding data sources, training methodologies, and potential biases inherent in the system.

4.1.4 Accountability and Responsibility: USNH including all students, staff, faculty, and affiliates, will be accountable and responsible for the development, deployment, and maintenance of AI systems used for official USNH business. Roles and responsibilities must be further defined by departments leveraging AI to ensure appropriate oversight, risk management, and adherence to this policy.

Any implementation of artificial intelligence is subject to USNH policies and standards, including the security review process. If you have questions about how to assess the above attributes for a given implementation of AI, please contact cybersecurity.grc@usnh.edu.

4.2 FAIRNESS AND BIAS

4.2.1 Avoiding Discrimination: USNH will strive to prevent unfair discrimination or bias in the development and use of AI systems. Bias mitigation techniques will be employed to address any inherent biases in training data or algorithms. Outcomes of generative AI are to be reviewed for bias, discrimination, and other hurtful content to ensure the respect of human rights, privacy, diversity, and inclusivity.

4.3 SECURITY AND SAFETY

4.3.1 Robustness and Reliability: AI systems must be developed with a focus on security and safety. Necessary measures must be taken to minimize the risks of data breaches, hacking, or misuse of AI systems.

4.3.2 Human Oversight: Human supervision must be maintained to ensure that AI systems operate within expected parameters. Fail-safe mechanisms must be in place to intervene or shut down AI systems if unintended behavior or risks are exhibited.

4.4 COLLABORATION AND INTERDISCIPLINARY RESEARCH

4.4.1 Collaboration: USNH encourages interdisciplinary collaboration in AI research, development, and implementation. Faculties and departments are encouraged to share knowledge, expertise, and resources to foster innovation and best practices.

4.4.2 Responsible AI Education: USNH Cybersecurity will provide AI education that emphasizes ethics, social impact, and responsible AI practices. Awareness campaigns and training sessions will be provided to educate staff, faculty, students, and affiliates about the implications and challenges of AI.

4.5 COMPLIANCE AND GOVERNANCE

4.5.1 Compliance with Laws and Regulations: USNH departments that leverage or develop AI systems must ensure all AI activities comply with relevant laws, regulations, and policies governing data protection, privacy, intellectual property rights, and ethical considerations.

4.5.2 Ethical Review: Ethical review boards or committees may be established to assess the potential ethical implications of AI research projects and to provide guidance on ethical best practices.

4.5.3 Continuous Improvement: USNH will regularly review and update this policy to reflect advancements in AI technology and evolving ethical considerations. Feedback from stakeholders and AI users will be actively sought by the USNH Cybersecurity Committee to improve guidelines and associated practices.

4.5.4 Regular Audits: Periodic audits and assessments of AI systems may be conducted to identify and rectify any biases or discriminatory outcomes. Regular audits may also be conducted to ensure AI systems are secure, functioning properly and within expected parameters.

5 CONCLUSION

This AI standard serves as a guiding framework for the responsible and ethical use of AI within the University System. By adhering to the principles outlined in this policy, the University System aims to foster an environment that promotes innovation, fairness, transparency, and accountability in AI research, development, and deployment.

For further cybersecurity and privacy guidance regarding Artificial Intelligence, USNH community members should refer to the National Institute of Standards and Technology (NIST) “Artificial Intelligence Risk Management Framework” or the NIST “Characteristics of Trustworthy AI” document.

6 MAINTENANCE OF THIS STANDARD

As part of the mandatory annual review of this Standard required by the USNH Cybersecurity Policy, the processes and procedures that support the requirements defined in this Standard shall be reviewed, and where needed, updated to ensure currency and continuous improvement.

University System of New Hampshire

7 ENFORCEMENT

Failure to comply with this Standard puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be proportionally appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units

8 EXCEPTIONS

Requests for exceptions to this Standard may be submitted and approved according to the requirements provided in the *Cybersecurity Exception Standard.*

9 DEFINITIONS

- Artificial Intelligence
- Generative AI

10 RELATED POLICIES AND STANDARDS

- USNH Information Classification Policy
- USNH Acceptable Use Policy
- USNH Privacy Policy
- USNH Cybersecurity Policy
- USNH Cybersecurity Exception Standard

11 CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question

University System of New Hampshire

12 DOCUMENT HISTORY

Effective Date:	31 JULY 2023
Approved by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, 31 JULY 2023, V1 USNH CYBERSECURITY COMMITTEE POLICY & STANDARD WORKING GROUP, 31 JULY 2023, V1
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, JULY 2023, V1 USNH CYBERSECURITY COMMITEE POLICY & STANDARD WORKING GROUP, JULY 2023, V1
Revision History:	REVIEW DRAFT FINALIZED, Dr. DAVID A YASENCHOCK, 31 JULY 2023