Responsible and Ethical Use of Artificial Intelligence (AI)

Policy Title:	Office of Internal Audit Responsible and Ethical Use of Artificial Intelligence (AI)
Policy Type:	Local
Policy Number:	04
Approval Date:	03/06/2026
Responsible Office:	Office of Internal Audit
Responsible Executive:	Chief Audit Executive
Applies to:	This policy applies to all employees, students, visitors, and contractors employed within or engaged by Norfolk State University's (NSU) Office of Internal Audit regardless of work location, including remote or hybrid environments, and to all university information technology and data, owned and operated by the university, or used for university business through contractual arrangements.

POLICY STATEMENT

All individuals to whom this policy applies shall comply with the NSU Information Security Policies and Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the NSU Information Security Policies and Standards.

Table of Contents

Responsible and Ethical Use of Artificial Intelligence (AI)

DEFINITIONS

Anonymized: Using a process to remove the association between identifying data and the data subject through a combination of masking and de-identification.

Artificial Intelligence (AI): The simulation of human intelligence processes by machines, especially computer systems, such that it can adapt and learn on its own using machine learning algorithms that can analyze large volumes of training data to identify correlations, patterns, and other metadata that can be used to develop a model that can make predictions or recommendations based on future data inputs.

AI Bias: AI Systems that systematically and unjustifiably yield less favorable, unfair, or harmful outcomes to members of specific demographic groups.

AI System: An engineered or machine-based artificial intelligence that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. They are designed to operate with varying levels of autonomy. AI Systems include solutions that exhibit Strong AI, such as Generative Artificial Intelligence, and Weak AI, such as Robotic Process Automation.

Data: Any form of information — structured or unstructured — that can be collected, stored, and processed for analysis or decision-making. In the context of generative AI tools, data is the input used to train, fine-tune, and guide models. It may include text, images, audio, video, code, or multimodal combinations.

COV AI System: An AI System that has been registered with Commonwealth Security and Risk Management (CSRM) and has been approved for use.

De-Identify/De-identification: The process of removing the association between a set of identifying data and the data subject. Thereby reducing the risk of identifying a data subject to a very small level by applying a set of data transformation techniques such that the resulting data retains very high analytic utility.

Intellectual Property: Please refer to the BOV POLICY #35 (2019) INTELLECTUAL PROPERTY POLICY.

Encryption/Encrypt: The process or the means of transforming plain text readable data into scrambled data that can only be deciphered with a cryptographic key, usually protected by a passphrase.

Generative Artificial Intelligence (Generative AI or GenAI): Systems that can create new content, such as text, images, music, or other digital content in response to prompts provided by its user. Generative AI models are trained on large datasets and use this knowledge to generate outputs that mimic or draw inspiration from their training examples.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Public AI Tools: Within the context of this policy, Publicly Available AI Tools refer to artificial intelligence systems, applications, or services that any individual can access via a self-service sign-up process without requiring an official contractual relationship with NSU. Examples of such tools

include, but are not limited to, platforms such as Personal ChatGPT, Personal Claude, and Personal Perplexity subscriptions. These tools are designed to process user-provided data and are not covered by enterprise-level agreements or dedicated support contracts with NSU.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled.

Sensitive Information/Data: Any data classified as sensitive under NSU Policy 32-02 – Data Classification Policy.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the university which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff, and students, as well as others who have been authorized to use NSU's technological resources, e.g. contractors, interns, volunteers, etc.

CONTACT(S)

The Office of Internal Audit (OIA) and the Office of Information Technology (OIT) officially interpret this policy. The Chief Audit Executive and the Chief Information Security Officer reserve the right to revise or eliminate this policy.

The OIA is responsible for maintaining any revisions as required by BOV Policy # 01 (2014) *Creating and Maintaining Policies* through the appropriate governance structures. Questions regarding this policy should be directed to OIA.

STAKEHOLDER(S)

Office of Internal Audit; Office of Information Technology; All others who have been authorized to use NSU's technological resources

PURPOSE

This policy establishes mandatory requirements to ensure the ethical, secure, and responsible use of AI within the Office of Internal Audit and to ensure violations are addressed through appropriate disciplinary or mitigation actions.

REQUIREMENTS

Securing AI Systems

- AI systems that generate content that could be harmful if misused must be protected against unauthorized access and tampering.
- AI systems must be fully tested to be secure and in line with privacy standards at all stages of the AI system life cycle.

- University data must not be shared with Generative AI tools, or Public AI Tools, unless part of an approved process.
- A feedback approach must be established to help ensure the trustworthiness of AI outputs (e.g., contents, decisions, etc.) and system performance.

AI Ethics

- Processes must be developed, reviewed, and approved prior to AI system or tool implementation to ensure all AI system use does not create or reinforce damaging AI biases.
- Mechanisms must be in place to ensure algorithmic-based decisions for AI-enabled systems and tools are transparent and can be explained by an authorized human.
- The appropriate multidisciplinary stakeholders must be identified and engaged in all AI system and tool strategy, requirements, testing, implementation, and maintenance to help ensure legal compliance, technical feasibility, and alignment with business and societal values.

AI Acceptable and Unacceptable Use

- Use of AI-enabled systems and tools must be limited to well-defined, legitimate purposes and comply with ethical and university policies and relevant external regulations and laws.
- AI-enabled systems must not be used to violate laws, compromise systems or users, internal or external to the university.
- Inappropriate use of AI-enabled systems and tools must be monitored and policy violations must be reported to the appropriate level of management (e.g., Chief Information Security Officer [CISO]).
- University information technology policies apply to AI-enabled systems and tools. This policy does not supersede or negate information technology policies or other university policies (e.g., information security, privacy, code of conduct, etc.).
- Examples of potential uses:
    - Audit Announcement Planning and Scoping Memo
    - Work Program Development
    - Executive Summary Development
    - Recommendation Analysis
    - Regulation Scanning and Monitoring
    - Policy Comparison
    - Fraud Detection

- Where these activities may involve sensitive or confidential data, only approved COV AI Systems or NSU-authorized tools may be used, and all data handling must comply with NSU data classification and security requirements.
- Users are responsible for understanding and remaining aware of the artificial intelligence capabilities of the software, applications, and technological resources they use, including existing, emerging, and evolving AI enabled functionality. Users shall review, manage, and appropriately configure available AI related controls and settings—including, but not limited to, data usage, retention, training, and sharing options—to ensure alignment with university policies and approved use. This responsibility applies regardless of whether AI functionality is

enabled by default or introduced through software updates. Where users require assistance or training to understand, verify, or configure AI related settings, they must consult the Office of Information Technology (OIT) or other designated university resources. Failure to appropriately manage AI related settings does not relieve users of responsibility for policy violations.

Data Handling and Training

- Data can only be used for training and testing AI systems if there is explicit permission from the data owner and if the use aligns with applicable personal data regulations.
- Sensitive and confidential data used for training and testing AI systems must be de-identified and anonymized to ensure privacy.
- Mechanisms must be established to ensure data quality and the accuracy and reliability of the generated output.

AI Transparency and Oversight

- AI-generated content that is shared or published is mandated to have the appropriate disclosures and/or other indicators (e.g., watermarks, inherent limitations of AI models, copyright, etc.).
- "Oversight for AI-enabled systems will be provided by the CISO, or a formally designated authority, with appropriate technical and governance expertise."

EDUCATION AND COMPLIANCE

This policy shall be published in the policy library and distributed to the Office of Internal Audit. To ensure timely publication and distribution thereof, the Office of Information Technology will make every effort to:

- Communicate this policy in writing, electronic or otherwise, to the Office of Internal Audit within 14 days of approval.
- Submit this policy for inclusion in the online Policy Library within 14 days of approval.
- Post this policy on the appropriate website.
- Educate and train all stakeholders and appropriate audiences on this policy's content, as necessary. Failure to meet the publication requirements does not invalidate this policy.
- Develop and maintain role-based training and awareness programs for NSU faculty, staff, and students, as well as any others who have been authorized to use NSU's technological resources on the responsible use of AI tools.

Reporting and investigation mechanisms must be established to ensure suspected violations of this policy are evaluated and appropriate action is taken.

Enforcement

Violations of this policy, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to university IT resources. In addition, failure to comply with requirements of this policy may result in disciplinary action up to and including termination or expulsion in accordance with relevant university policies, and may violate federal, state, or local laws.

Exceptions

Exceptions to this policy must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Audit Executive, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: 03/06/2029
- Approval by: Audit, Risk Compliance Committee
- Revision History: N/A
- Supersedes: N/A

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx

32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx

38-10 - Information Security Policy
https://www.nsu.edu/policy/bov-38-10.aspx

Virginia Department of Human Resources Management Policy 1.75
Virginia Department of Human Resources Management Policy 1.75

VITA AI Policy Standards and IT Standards
https://www.vita.virginia.gov/policy--governance/governance/artificial-intelligence/